SILVERNET

WIRELESS-NETWORK-SOLUTIONS

SIL WAC AX

User Manual

TABLE OF CONTENTS

INTRODUCTION

This User Guide is for the SilverNet SIL WAC AX AC controller.

SUPPORTED PRODUCTS

The SIL WAC AX supports the following products:

• SIL WCAP-AX

• SIL WCAP-AX-W

• SIL WCAP-AX-EXT

• SIL WCAP-AX-EXT+

For more information, visit **www.silvernet.com**

WIRELESS MODES

The SilverNet Access Points support the following modes:

• FAT mode

A FAT AP can provide wireless access independently.

• FIT mode

A FIT AP must be used with a controller to provide wireless access.

SYSTEM REQUIREMENTS

• Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10, Linux, or Mac OS X

• Web Browser: Mozilla Firefox, Apple Safari, Google Chrome, or Microsoft Internet Explorer 9 (or above)

PACKING LIST

Please check the following items in the package before installing the device

AC Controller	1 piece
User manual	1 copy
Powe Cable	1 piece
Set of brackets	1 piece
Set of screws	1 piece

Please contact your distributor immediately for any missing or damaged items.

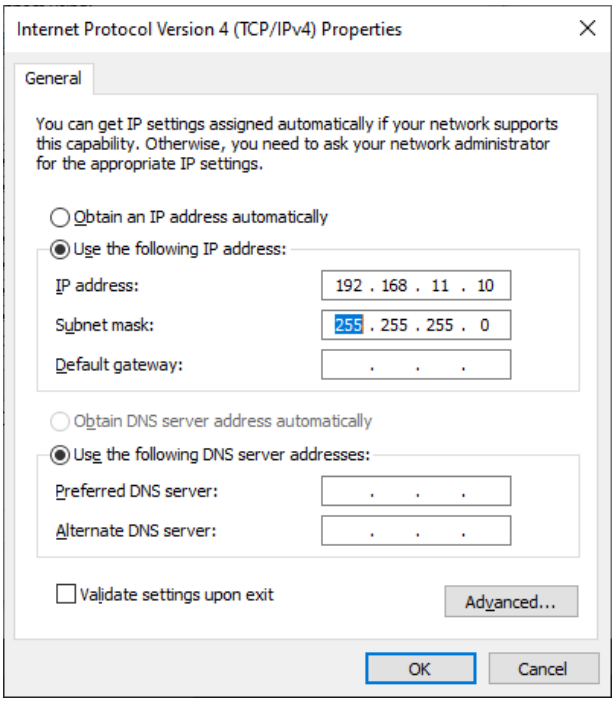
CONFIGURATION

GETTING STARTED

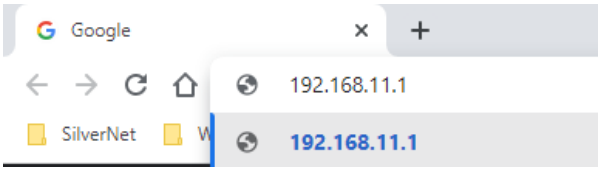
The Controller is sent out on DHCP. Once you have connected the controller to your network it is recommended you run an IP scan to check the IP address. If no DHCP server is available, then the controller will either be on 192.168.1.2 or 192.168.11.1

To access the Controllers Configuration Interface, perform the following steps:

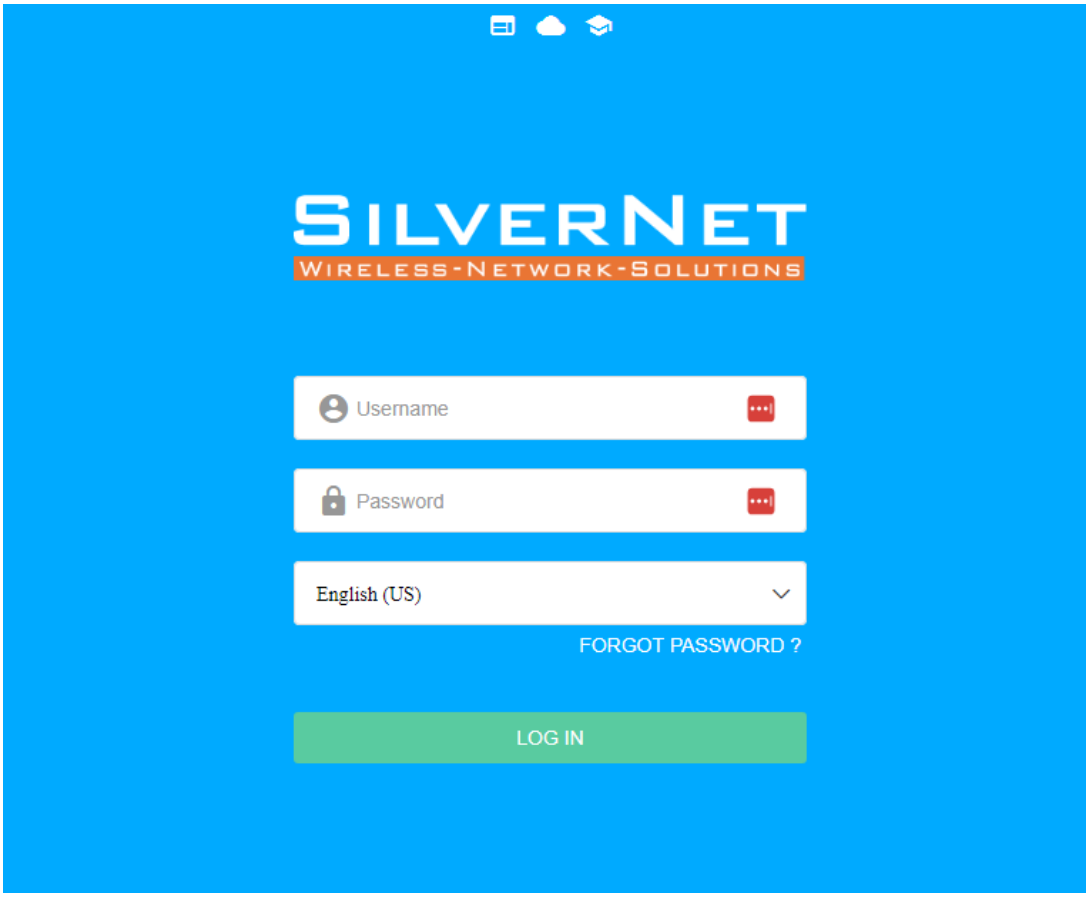
1. Configure the Ethernet adapter on your computer with a static IP address on the correct subnet. In this example we will be using the 192.168.11.x subnet (for example, IP address: 192.168.11.10 and subnet mask: 255.255.255.0)



2. Launch your web browser and enter the IP address of the controller into the address field. The SIL WAC AX has a default IP address of either 192.168.1.2 or 192.168.11.1



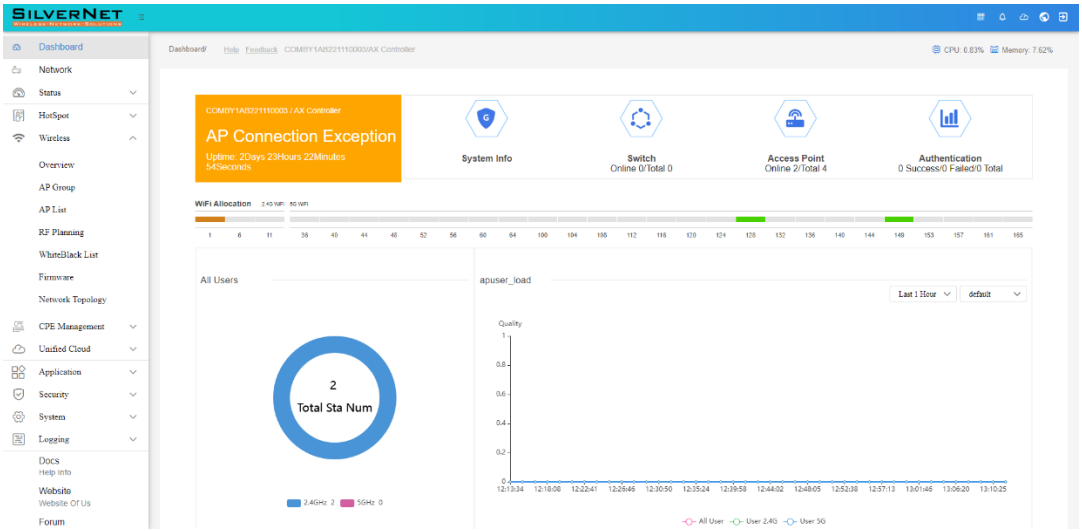
3. Enter **admin** in the Username field and **admin** in the Password field and click **Login**.



SYSTEM OVERVIEW

DASHBOARD

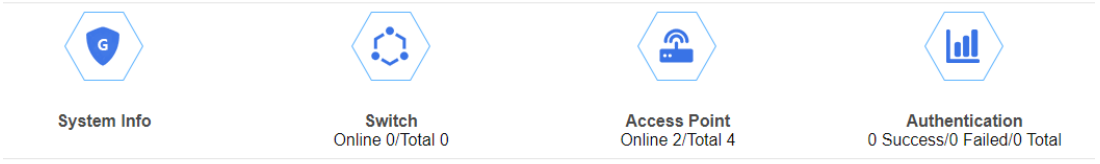
The Dashboard displays a summary of the controller status information, Total number of users, AP load and online devices.



NETWORK STATUS

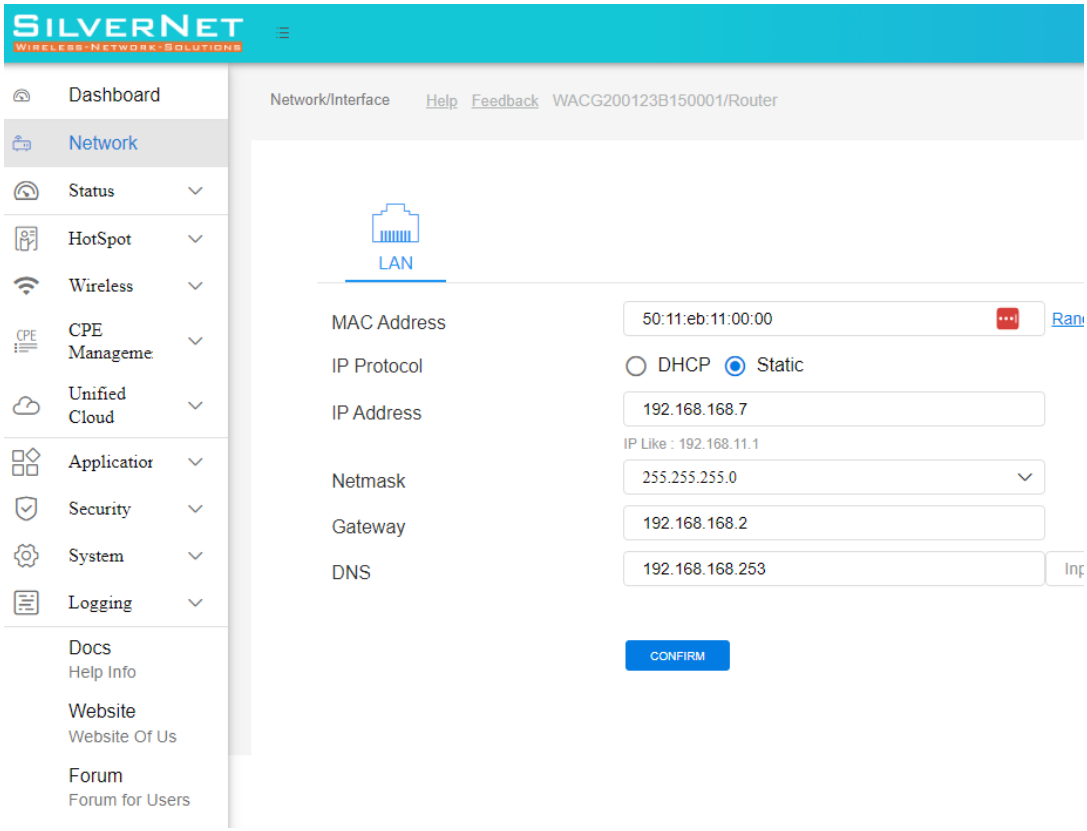
You can check some basic system info, get some information on the connected AP's and Authentication by hovering your mouse over the blue icons and by clicking them.

The pages they open will be covered later in the manual.



NETWORK

Click on the network tab to configure the IP address of the controller.



General Setup

IP Protocol Here you can enable **DHCP Client** or **Static**

DHCP Client If enabled, your device will get an IP address automatically from the network. There must be a DHCP server configured on your network for this to function.

Static Allows you to enter a static IP address.

IP Address Enter the IP address you wish to give to the device. You will use this IP address to access the device interface.

Netmask Enter the class for the IP address. The default is a class C value of 255.255.255.0

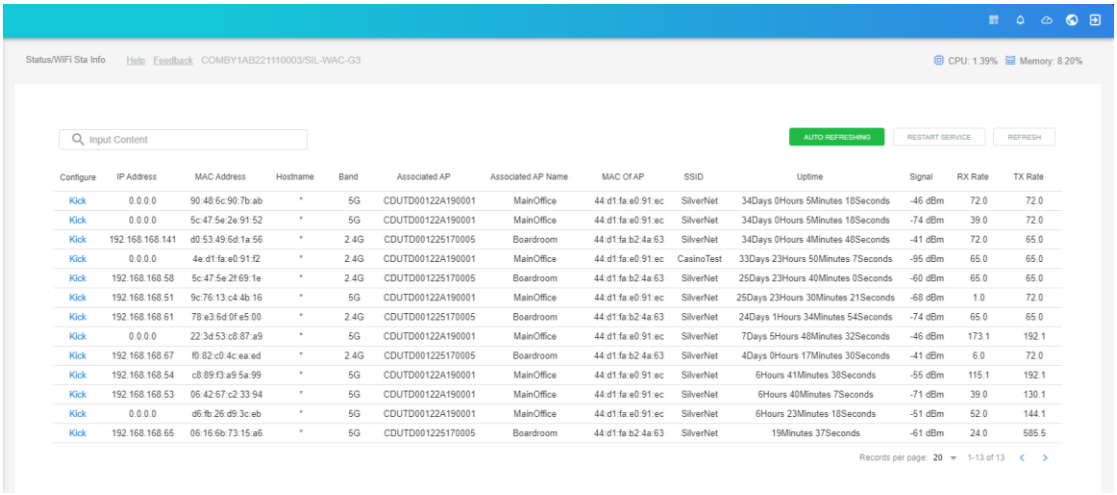
Gateway (optional) Enter the gateway IP address of the network the device is connected to.

DNS Enter the IP address for the DNS server you wish to use.

STATUS

WIFI STA INFO

Click on WiFi Sta Info for a detailed list of connected end users.



Configure	IP Address	MAC Address	Hostname	Band	Associated AP	Associated AP Name	MAC Of AP	SSID	Uptime	Signal	RX Rate	TX Rate
Kick	0.0.0.0	90:48:6c:90:7b:ab	*	5G	CDUTD00122A190001	MainOffice	44:d1:fa:e0:91:ec	SilverNet	34Days 0Hours 5Minutes 18Seconds	-46 dBm	72.0	72.0
Kick	0.0.0.0	5c:47:5e:2e:91:52	*	5G	CDUTD00122A190001	MainOffice	44:d1:fa:e0:91:ec	SilverNet	34Days 0Hours 5Minutes 18Seconds	-74 dBm	39.0	72.0
Kick	192.168.168.141	d0:53:49:6d:1a:56	*	2.4G	CDUTD001225170005	Boardroom	44:d1:fa:b2:4a:63	SilverNet	34Days 0Hours 4Minutes 48Seconds	-41 dBm	72.0	65.0
Kick	0.0.0.0	4e:d1:fa:e0:91:f2	*	2.4G	CDUTD00122A190001	MainOffice	44:d1:fa:e0:91:ec	CasinoTest	33Days 23Hours 50Minutes 7Seconds	-95 dBm	65.0	65.0
Kick	192.168.168.58	5c:47:5e:2f:69:1e	*	2.4G	CDUTD001225170005	Boardroom	44:d1:fa:b2:4a:63	SilverNet	25Days 23Hours 40Minutes 0Seconds	-60 dBm	65.0	65.0
Kick	192.168.168.51	9c:76:13:c4:4b:16	*	5G	CDUTD00122A190001	MainOffice	44:d1:fa:e0:91:ec	SilverNet	25Days 23Hours 30Minutes 21Seconds	-68 dBm	1.0	72.0
Kick	192.168.168.61	78:e3:6d:0f:e5:00	*	2.4G	CDUTD001225170005	Boardroom	44:d1:fa:b2:4a:63	SilverNet	24Days 1Hours 34Minutes 54Seconds	-74 dBm	65.0	65.0
Kick	0.0.0.0	22:3d:53:c8:87:a9	*	5G	CDUTD00122A190001	MainOffice	44:d1:fa:e0:91:ec	SilverNet	7Days 5Hours 48Minutes 32Seconds	-46 dBm	173.1	192.1
Kick	192.168.168.67	f0:82:c0:4c:ea:ed	*	2.4G	CDUTD001225170005	Boardroom	44:d1:fa:b2:4a:63	SilverNet	4Days 0Hours 17Minutes 30Seconds	-41 dBm	6.0	72.0
Kick	192.168.168.54	c8:89:f3:a9:5a:99	*	5G	CDUTD00122A190001	MainOffice	44:d1:fa:e0:91:ec	SilverNet	6Hours 41Minutes 38Seconds	-55 dBm	115.1	192.1
Kick	192.168.168.53	06:42:67:c2:33:94	*	5G	CDUTD00122A190001	MainOffice	44:d1:fa:e0:91:ec	SilverNet	6Hours 40Minutes 7Seconds	-71 dBm	39.0	130.1
Kick	0.0.0.0	d6:fb:26:d9:3c:eb	*	5G	CDUTD00122A190001	MainOffice	44:d1:fa:e0:91:ec	SilverNet	6Hours 23Minutes 18Seconds	-51 dBm	52.0	144.1
Kick	192.168.168.65	06:16:6b:73:15:a6	*	5G	CDUTD001225170005	Boardroom	44:d1:fa:b2:4a:63	SilverNet	19Minutes 37Seconds	-61 dBm	24.0	585.5

Records per page: 20 1-13 of 13

Configure Clicking Kick will disconnect the end user device for a short period of time, after which the user can reconnect.

IP Address The IP address of the end user device.

MAC address The MAC address of the end user device.

Host Name The name of the end user device.

Associated AP The name of the AP that the end user is connected to.

MAC of AP The MAC address of the AP that the end user is connected to.

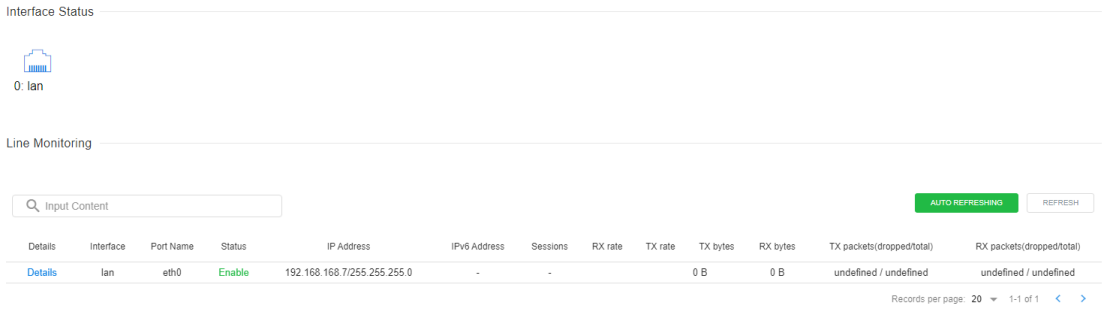
SSID The SSID name of the wireless connection the end user is connected to.

Uptime The network connection time of the end user.

Signal The current signal strength of the end users connection to the AP.

RX/TX rate The connection rate of the wireless device.

LINE MONITORING



Details Click details to view the line monitoring details.

Interface The name of the selected interface.

Port Name The name of the selected port.

Status Green is Enabled and red is Disabled.

IP address The IP address of the selected interface.

IPV6 Address The IPv6 address of the selected interface.

Sessions The number of sessions.

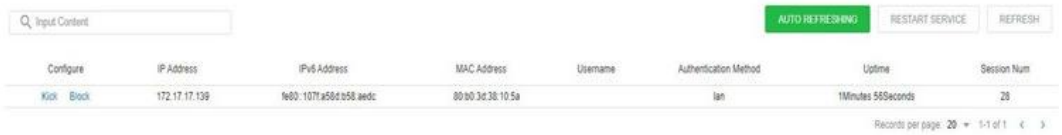
RX/TX rate The connection rate of the selected interface.

RX/TX bytes The volume of data, in bytes, transmitted via the selected interface.

RX/TX packets The dropped and total packets of the selected interface.

AUTHORISED USERS

A list of authenticated users that have connected via the portal.



Configure Clicking Kick will disconnect the end user device. The user will need to re-authenticate to access the internet. Clicking Block will Move the end user device to the Blacklist and block the device from connecting to the network.

***You can remove a user from the Blacklist by going to HotSpot-Blacklist**

IP Address The IP address of the end user device.

IPv6 Address The IPv6 address of the end user device.

MAC address The MAC address of the end user device.

Host Name The name of the end user device.

Authentication Method The Method of authentication.

Uptime The network connection time of the end user.

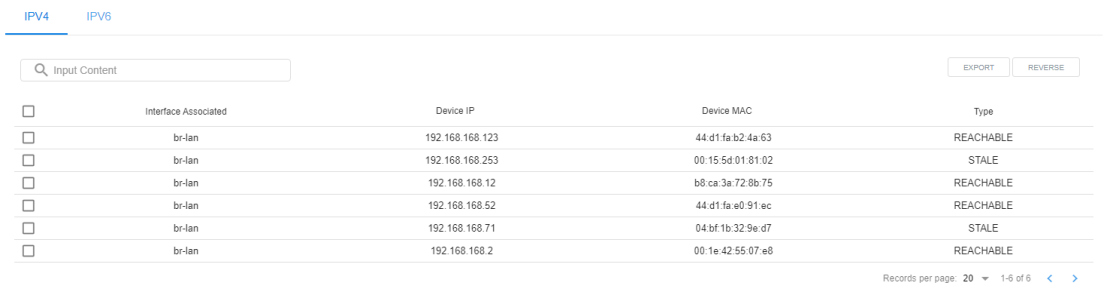
Session Number The session number of the end user.

License

Here you can view the license information of the controller.

ARP List

ARP (address Resolution Protocol) is a TCP/IP protocol that connects a physical address to an IP address. When a computer or mobile phone sends a message, it broadcasts the ARP request containing the target IP address to all devices on the local network. One it receives a reply it will then be able to determine the target physical address and will store the information in the local ARP cache for a period of time. This will save time for any future requests as it will query the ARP cache first.



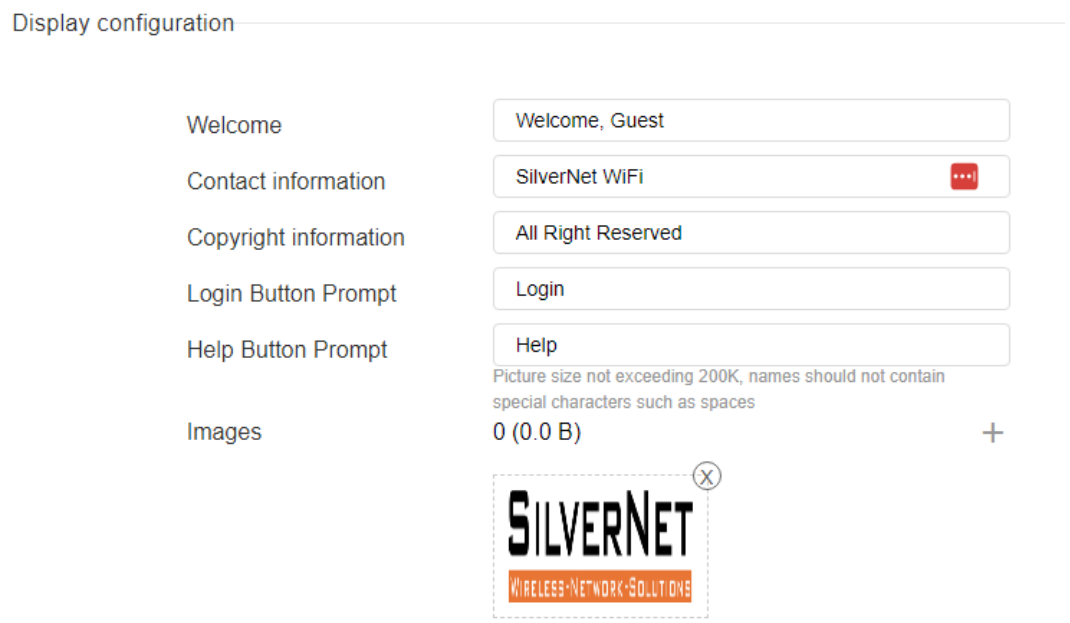
HOTSPOT

This is where you can create a guest network with varied levels of authentication and billing plans.

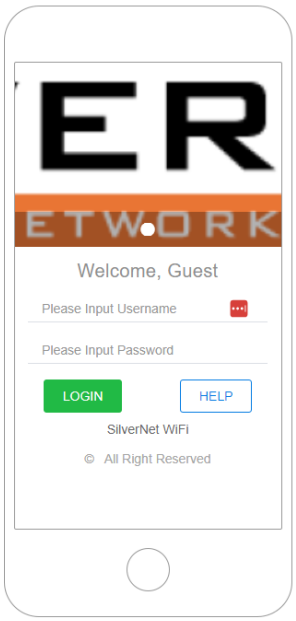
LOCAL PORTAL

Here you can enter the details for your landing display.

DISPLAY CONFIGURATION

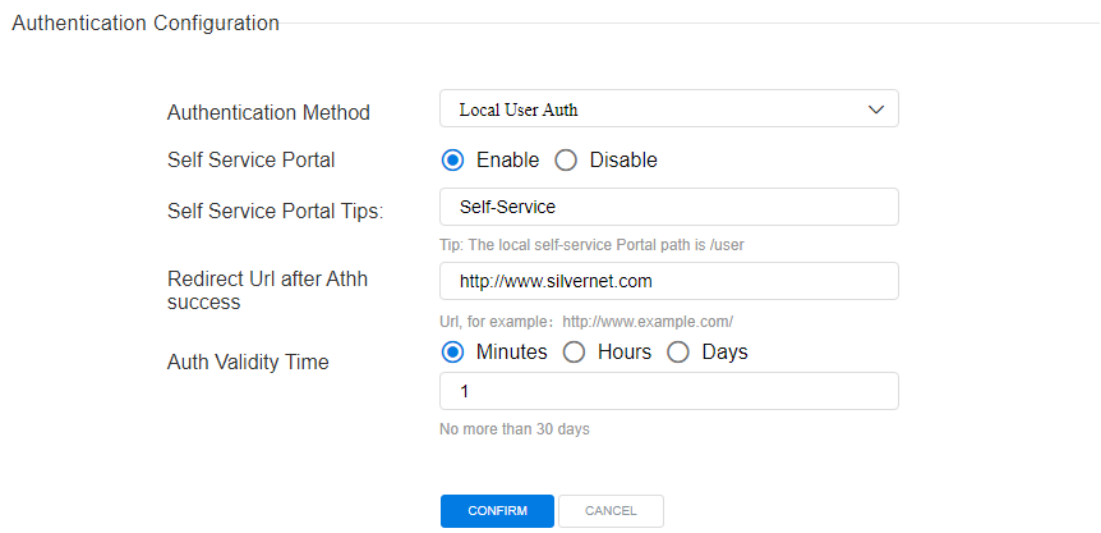


This phone image will show you a preview of what the display will look like.



AUTHENTICATION CONFIGURATION – LOCAL USER

Here you can configure the Authentication method.



Authentication Method Local User Authentication.

Self Service Portal Enable or Disable. We recommend to disable.

Self Service Portal Tips Self service button tips.

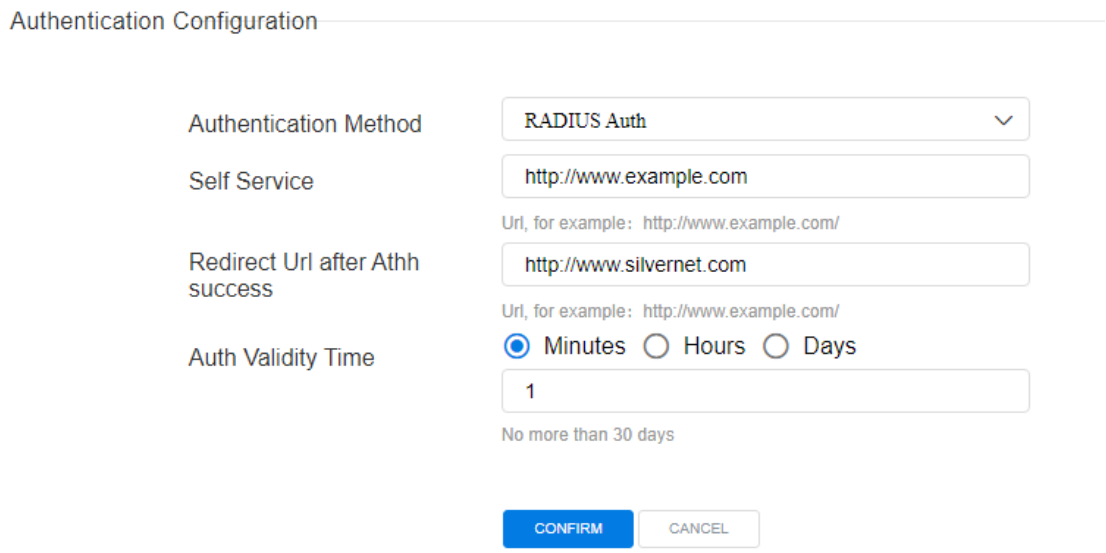
*Self Service portal is where the customer can go through to a webpage, create and accounts and purchase additional internet time themselves. The account will show in local users.

Redirect URL after Authentication Success Enter the URL of the landing page once the user is authenticated.

Authentication validity Time The amount of time the users session is valid for.

AUTHENTICATION CONFIGURATION – RADIUS AUTH

Here you can configure the Authentication method.

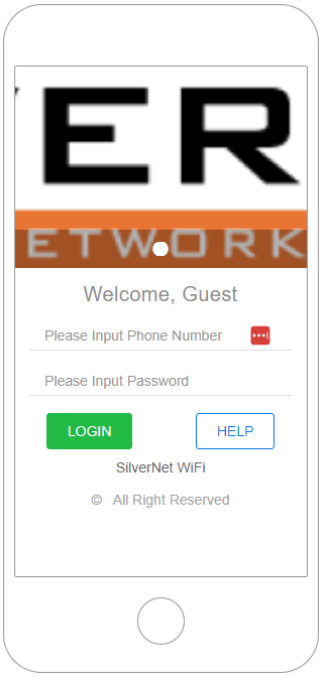


Authentication Method RADIUS Auth.

Self Service Enter the Self Service URL.

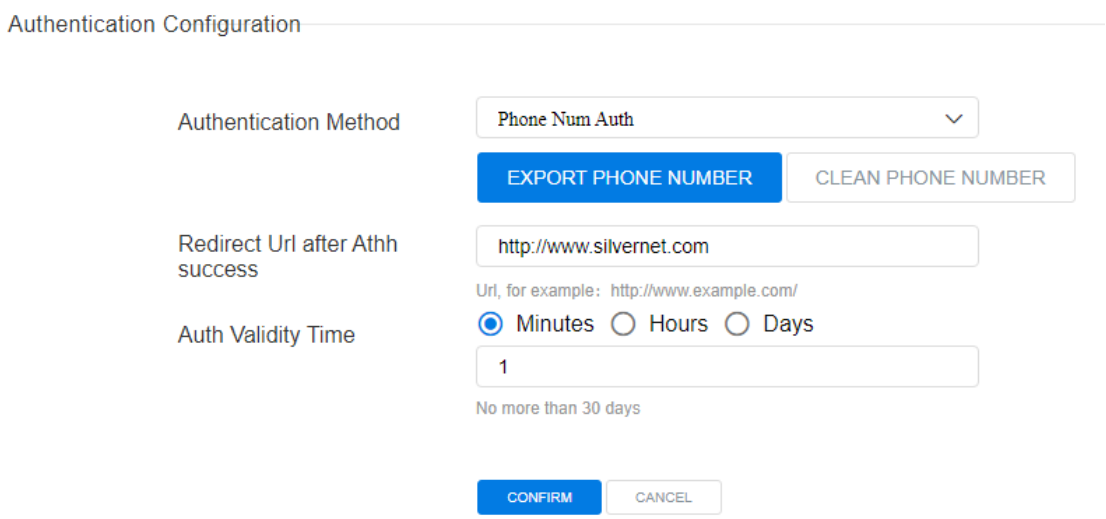
Redirect URL after Athh success Enter the URL of the landing page once the user is authenticated.

Authentication validity Time The amount of time the users session is valid for.



AUTHENTICATION CONFIGURATION – PHONE NUM AUTH

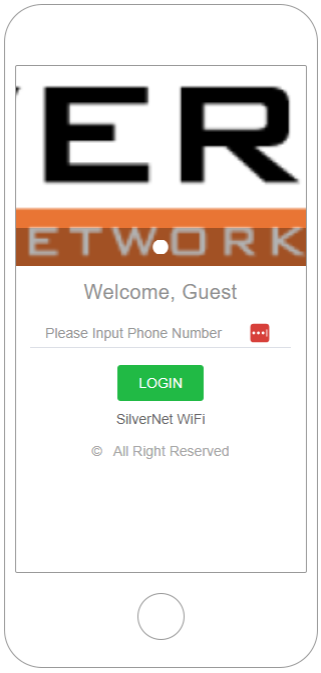
Here you can configure the Authentication method.



Authentication Method Phone Num Auth.

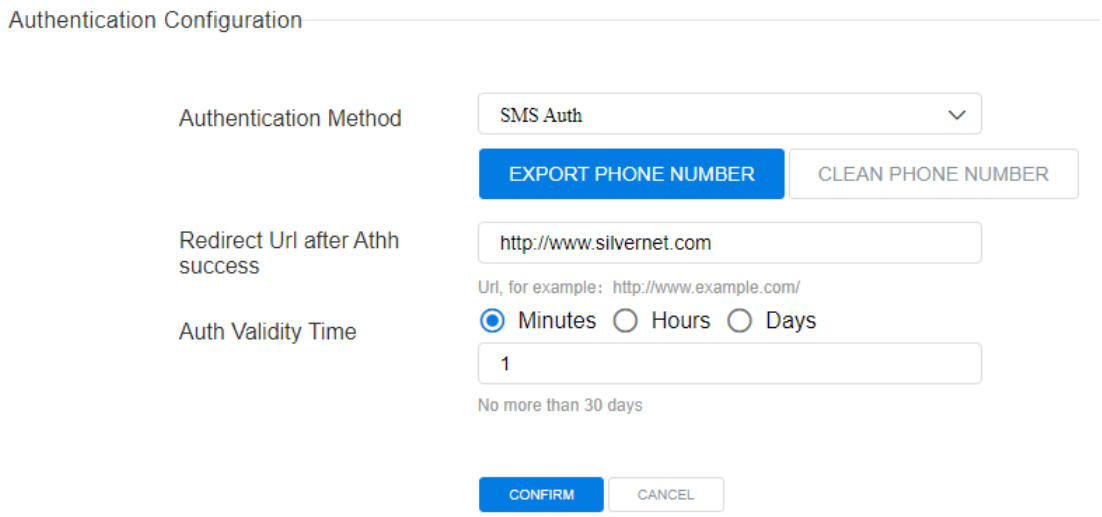
Redirect URL after Athh success Enter the URL of the landing page once the user is authenticated.

Authentication validity Time The amount of time the users session is valid for.



AUTHENTICATION CONFIGURATION – SMS AUTH

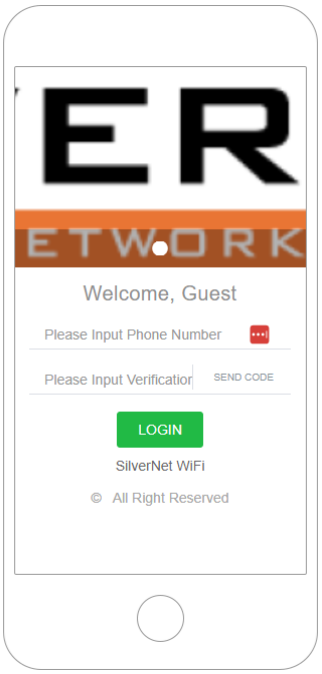
Here you can configure the Authentication method.



Authentication Method SMS Auth.

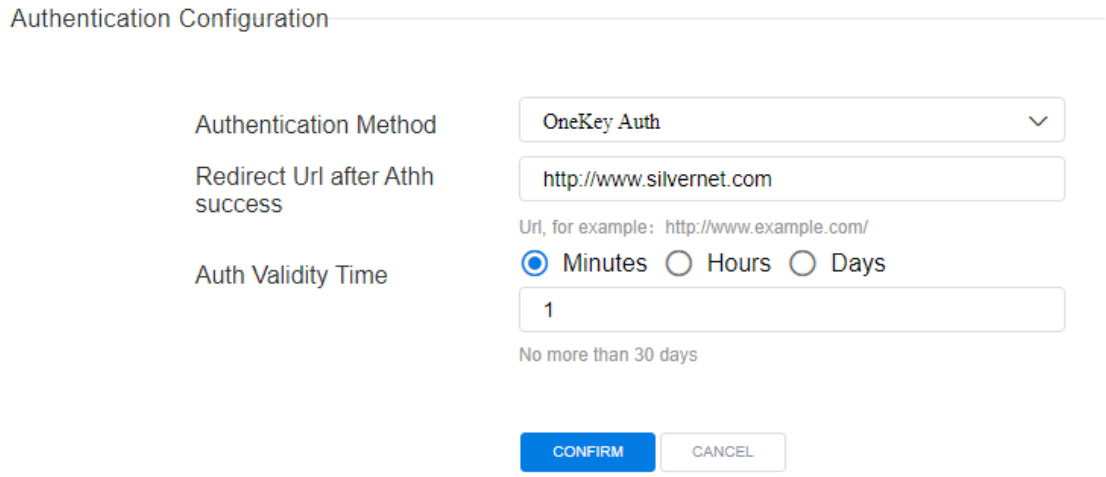
Redirect URL after Athh success Enter the URL of the landing page once the user is authenticated.

Authentication validity Time The amount of time the users session is valid for.



AUTHENTICATION CONFIGURATION – ONEKEY AUTH

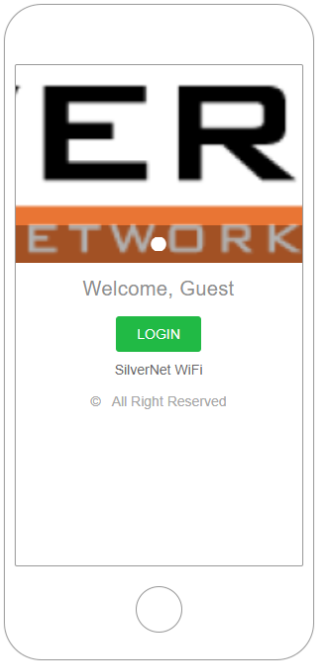
Here you can configure the Authentication method.



Authentication Method OneKey Auth.

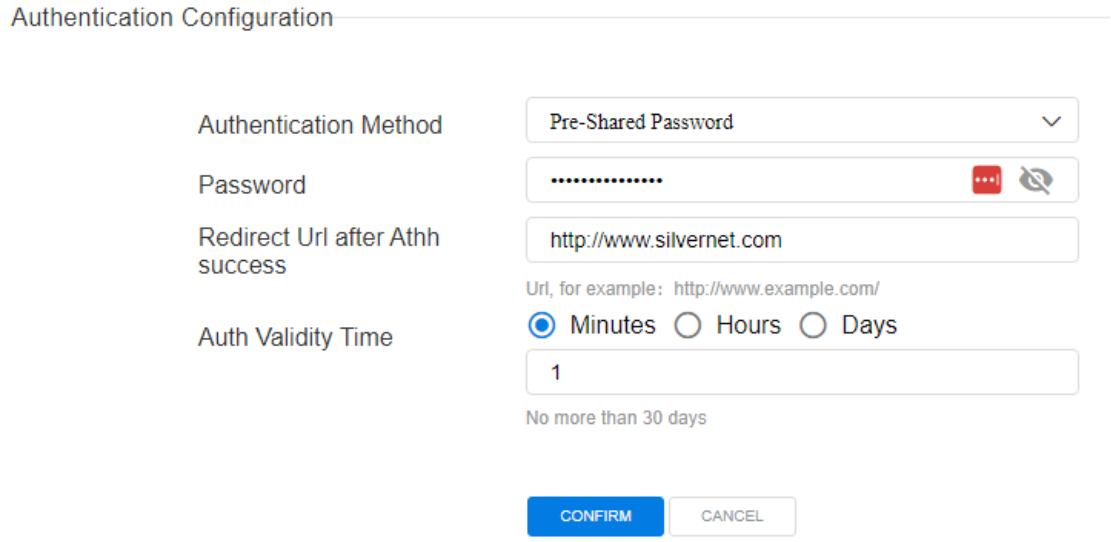
Redirect URL after Athh success Enter the URL of the landing page once the user is authenticated.

Authentication validity Time The amount of time the users session is valid for.



AUTHENTICATION CONFIGURATION – PRE-SHARED PASSWORD

Here you can configure the Authentication method.

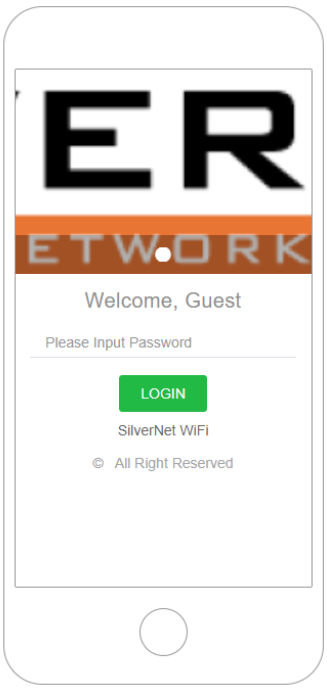


Authentication Method Pre-Shared Password.

Password Enter the Pre-Shared Password.

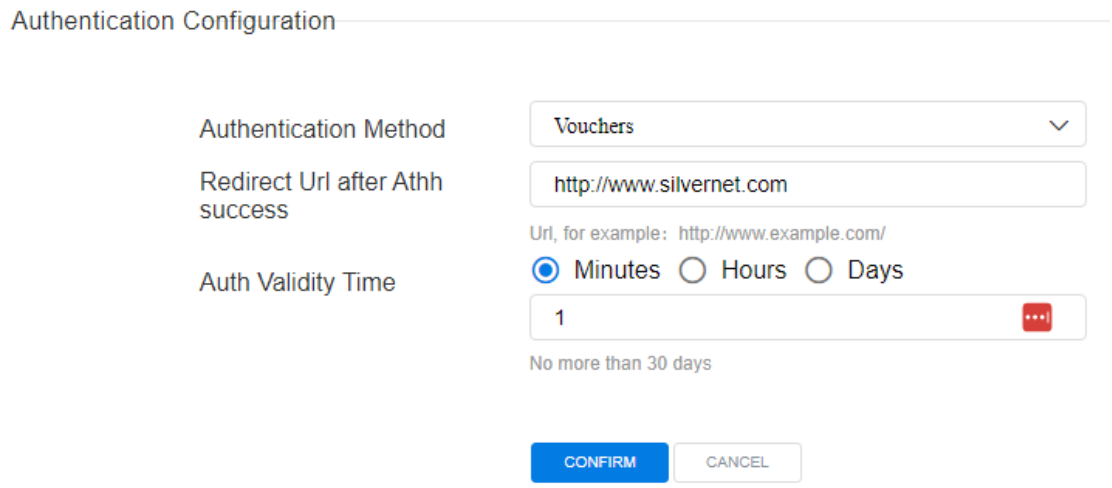
Redirect URL after Athh success Enter the URL of the landing page once the user is authenticated.

Authentication validity Time The amount of time the users session is valid for.



AUTHENTICATION CONFIGURATION – VOUCHERS

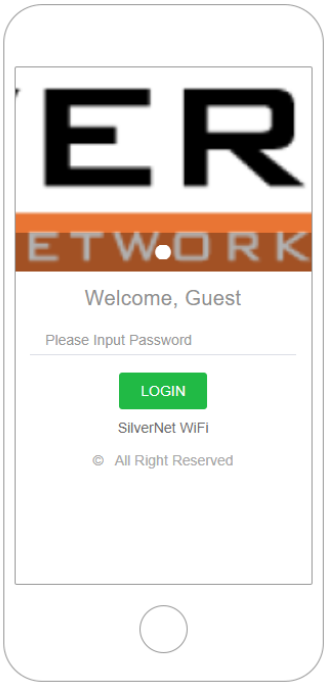
Here you can configure the Authentication method.



Authentication Method Vouchers.

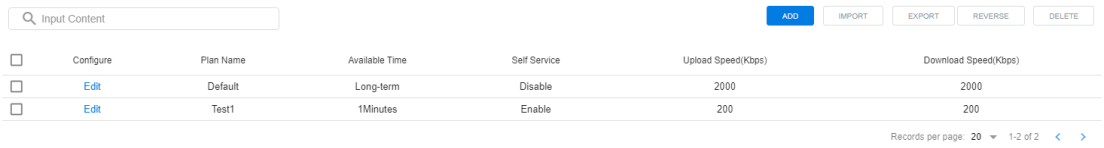
Redirect URL after Athh success Enter the URL of the landing page once the user is authenticated.

Authentication validity Time The amount of time the users session is valid for.

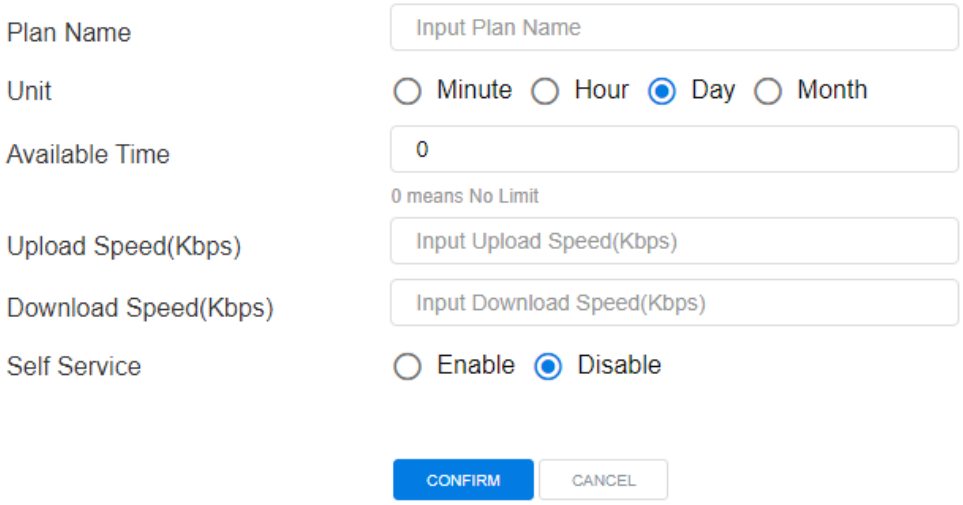


BILLING PLAN

Billing plan is used with Local Portal.



Click the Add button to add a new billing plan.



Plan Name Enter the name of the billing plan.

Unit Select the unit of time.

Available Time Set the Time limit. 0 means there is no limit.

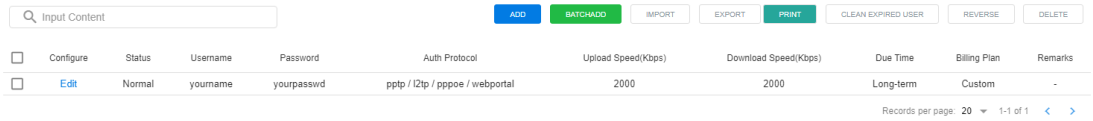
Upload Speed (Kbps) Enter the upload speed limit in Kbps.

Download Speed (Kbps) Enter the download speed limit in Kbps.

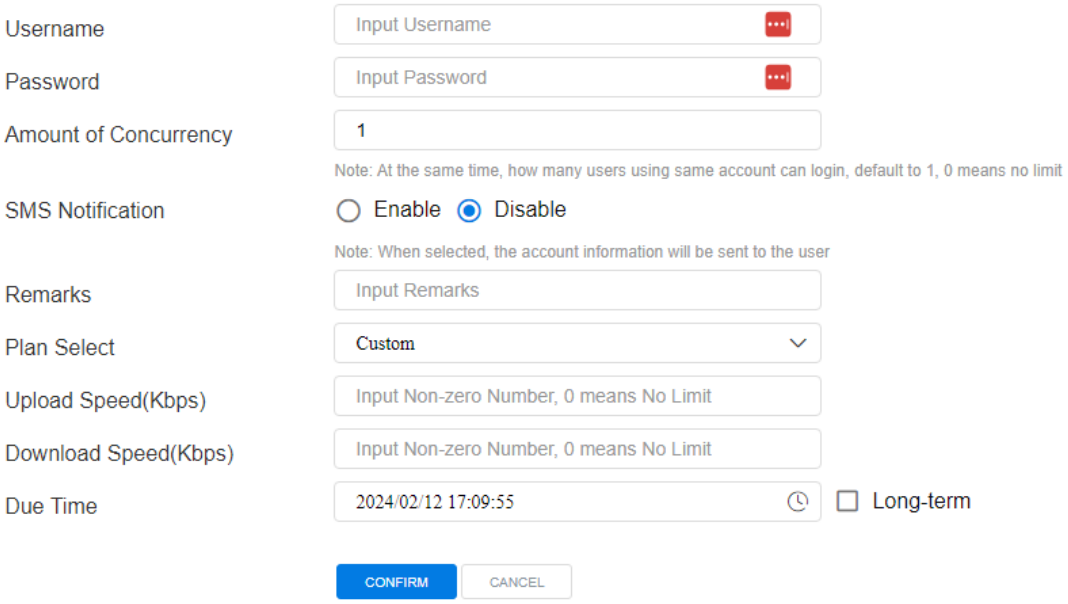
Self Service Enable or Disable.

LOCAL USERS

This is where you can set up a general login, Local users or long term guests.



Click Add or edit to begin making changes.



Username Enter a username.

Password Enter a password.

Amount of Concurrency Set the maximum number of users that are allowed to login at the same time on the same account. 0 means there is no limit.

SMS Notification Enable or Disable. If enabled will need to configure SMS Gateway.

Remarks Add a remark.

Plan Select You can select any template that you have created in the Billing Plan section.

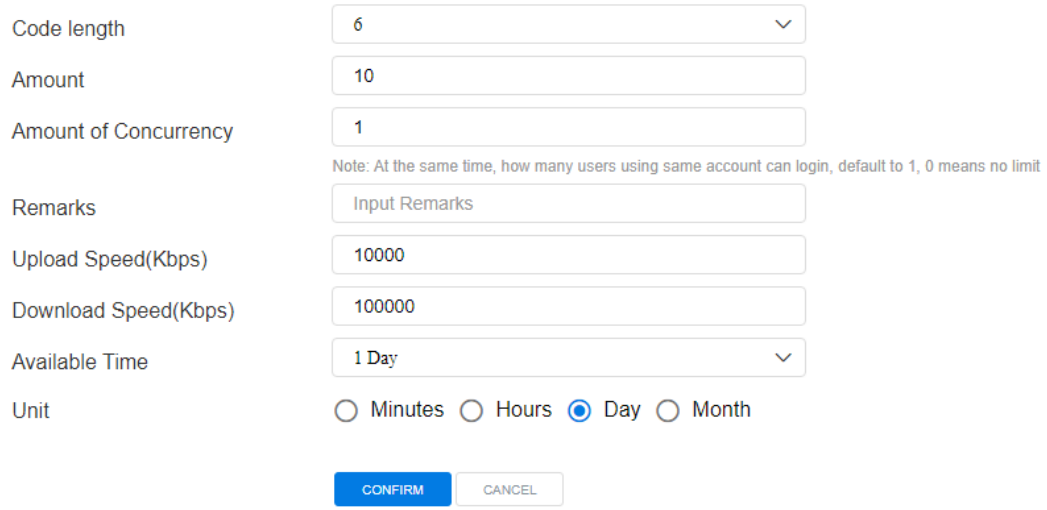
Upload/Download Speed (Kbps) Enter the upload/download speed limit in Kbps. If using a template it will follow template rules.

Due Time This is the expiry time of the account. Click long term to disable the expiry.

VOUCHERS

This is where you can create vouchers for end users. Ideal for a Hotel scenario.

Click Batch Add.



Code Length This will be the length of the code.

Amount Enter the amount of vouchers you wish to populate.

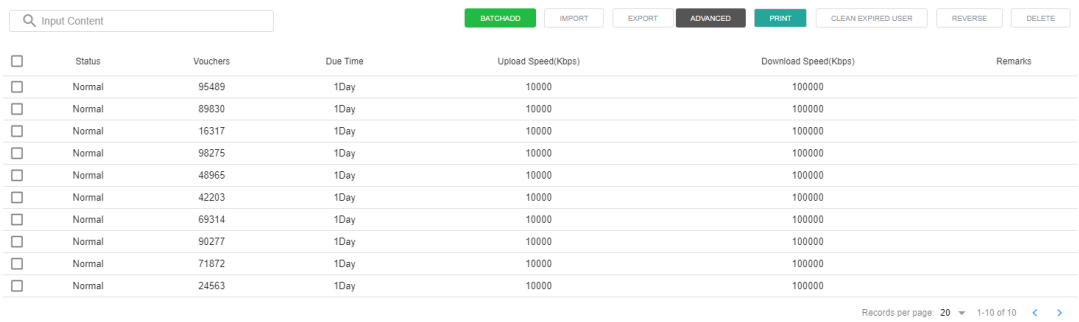
Amount of Concurrency Set the maximum number of users that are allowed to login at the same time on the same account. 0 means there is no limit.

Remarks Add a remark.

Upload/Download Speed (Kbps) Enter the upload/download speed limit in Kbps.

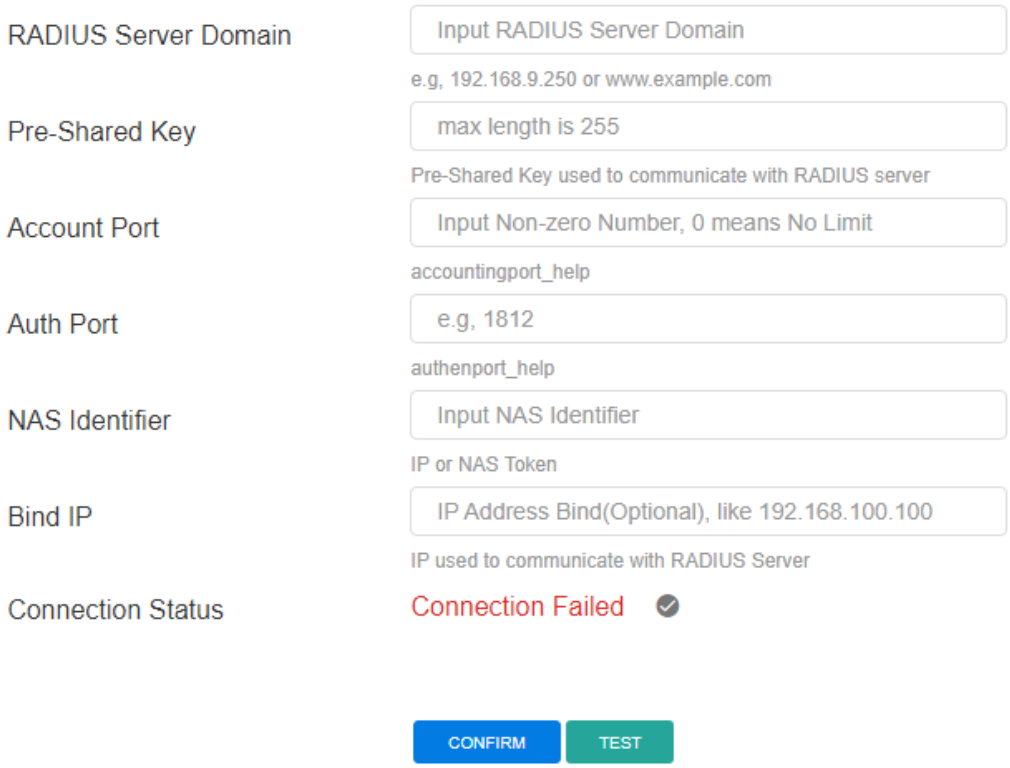
Available Time/Unit This is the length of the voucher.

Once confirmed the list will appear as below.



RADIUS

This is where you can set up Radius Authentication.



Radius Server Domain Enter your Radius server IP address.

Pre-Shared Key Enter the Radius server Pre-Shared Key.

Account Port Enter the Radius server account port number.

Auth Port Enter the Radius server Authentication port number.

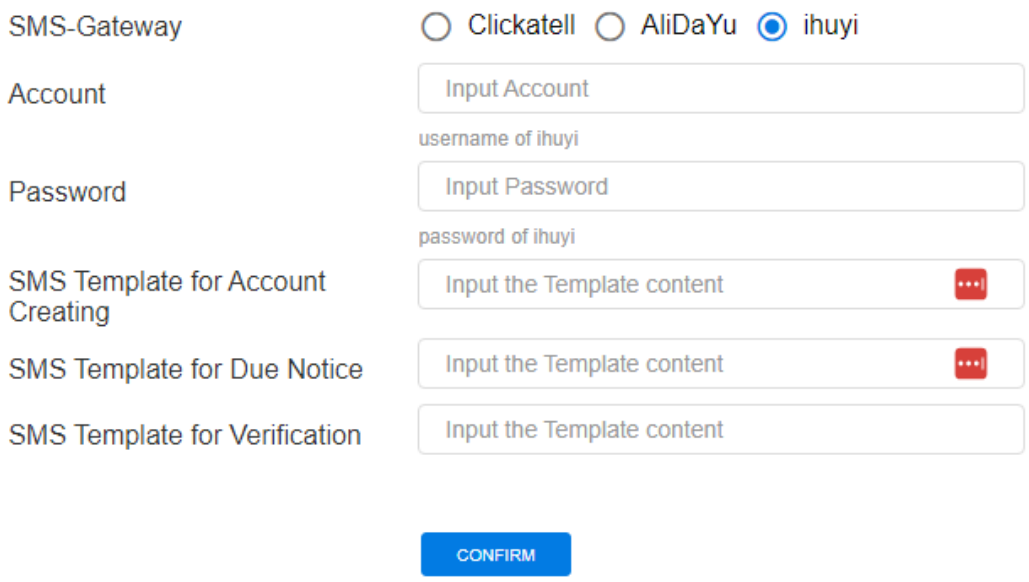
NAS Identifier IP address of the network access server (NAS) that requests user authentication.

Bind IP Optional IP address to Bind to.

Once the information has been entered you can test the connection and then confirm.

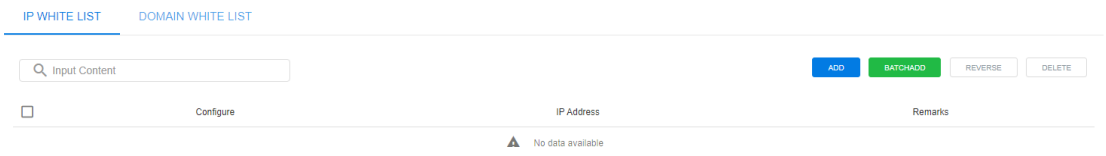
SMS Gateway

This is where you can select the SMS Gateway. Currently we only support Clickatell, AliDaYu and Ihuyi.



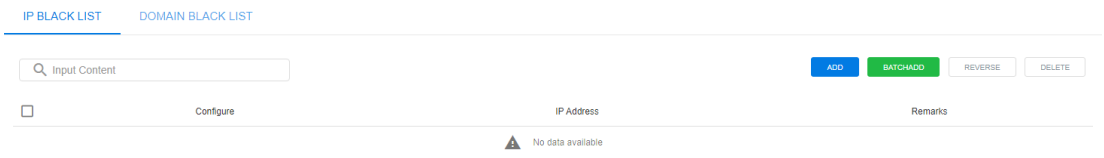
Enter your account details to enable SMS.

White List



Select IP or Domain white list, and click the add or batch add button to fill in address. Any IP entered here will not need to Authenticate.

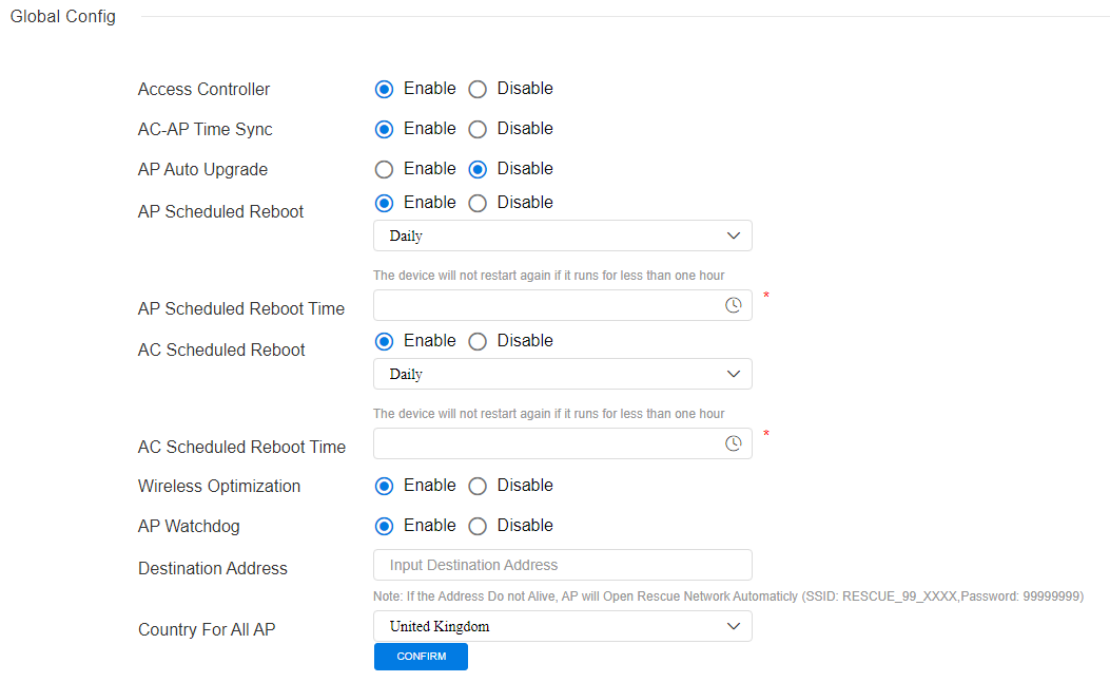
Black List



Select IP or Domain Black list, and click the add or batch add button to fill in address. Any Ip address entered here will not be able to access the network.

WIRELESS

OVERVIEW



Access Controller Select Enable or Disable.

AC-AP Time Sync Select Enable or Disable.

AP Auto Upgrade Select Enable or Disable.

AP Scheduled Reboot Select Enable or Disable. If Enabled, select if the schedule will be Daily, Weekly or Monthly and then Select the Day of the week or Month.

AP Scheduled Reboot Time Select the time you wish the AP's to be rebooted.

AC Scheduled Reboot Select Enable or Disable. If Enabled, select if the schedule will be Daily, Weekly or Monthly and then Select the Day of the week or Month.

AC Scheduled Reboot Time Select the time you wish the AC to be rebooted.

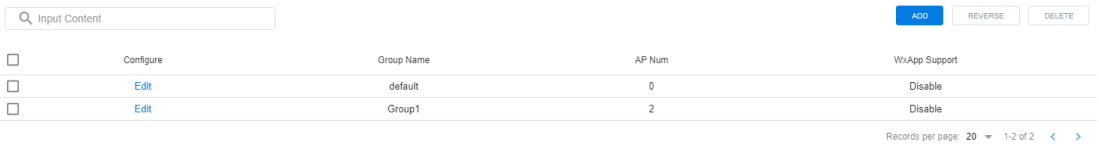
Wireless Optimisation Select Enable or Disable.

AP Watchdog Select Enable or Disable. Input the address of the AP's you wish to monitor. If the AP is offline it will go into rescue mode with details of (SSID: RESCUE_99_XXXX,Password: 99999999)

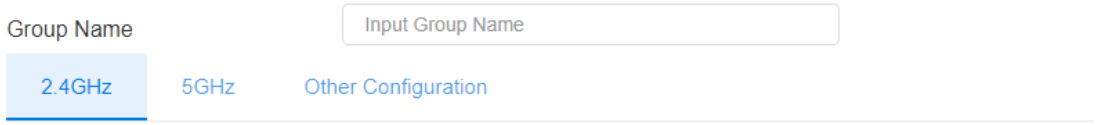
Country For All AP Select the country code you wish to use.

AP Group

This is where you can create AP groups



Click the Add button to add a group or edit to edit a current group.

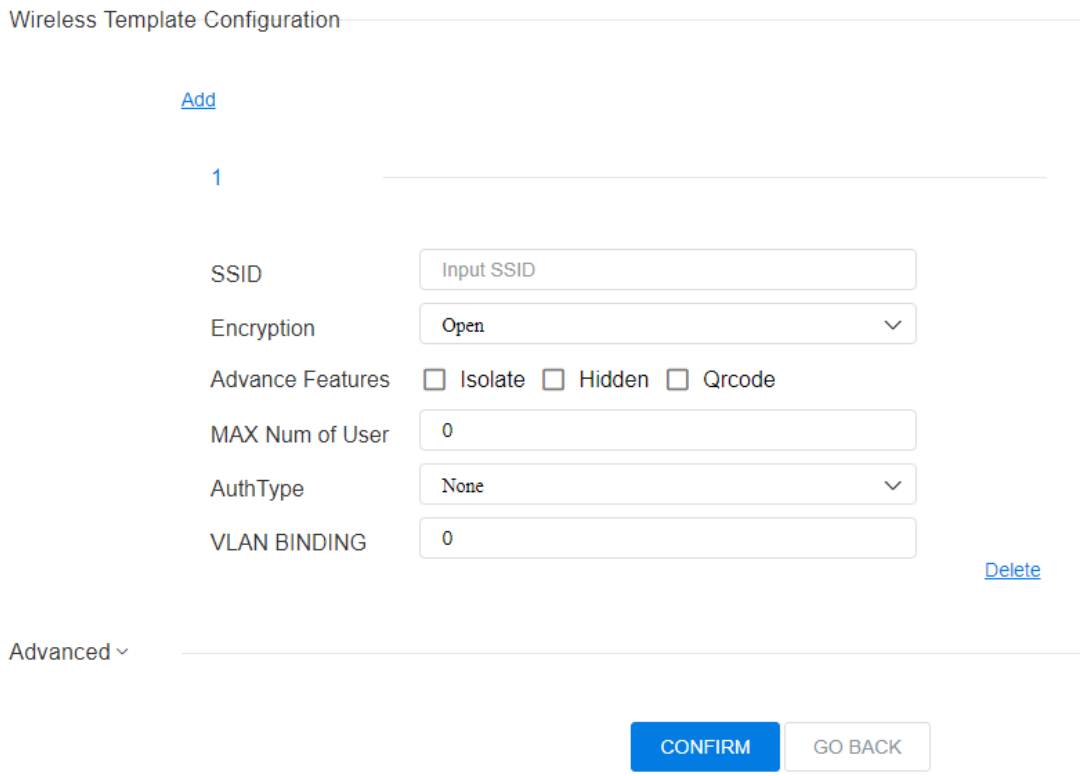


Group Name Enter a name for the Group.

Select 2.4GHz, 5GHz or Other configuration to edit those settings.

2.4GHz

Configure your 2.4Ghz settings.



SSID Enter the SSID. This will be visible to other devices.

Encryption Select your encryption method.

Advanced features Select if needed. **Isolate** will stop any user devices connected to this Wi-Fi from communicating with each other. **Hidden** will hide the SSID so that it is not visible.

Max Num of User Enter the maximum number of users or leave at 0 for unlimited.

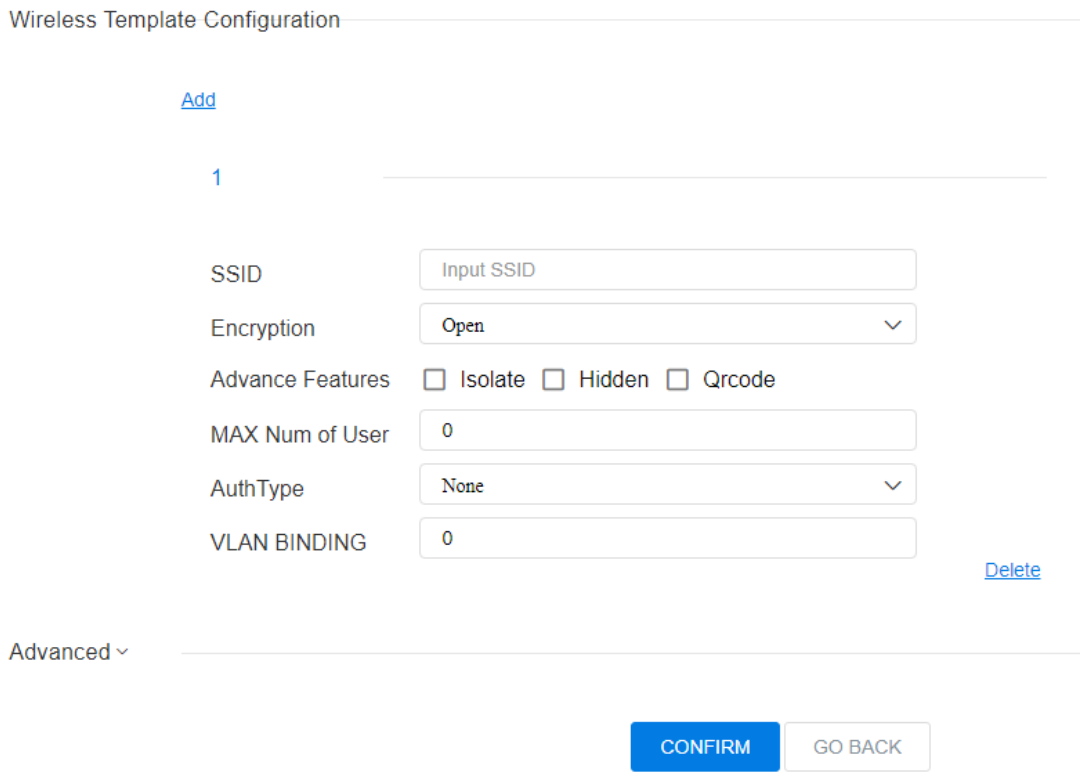
Authentication Type Select None or Local Portal.

VLAN Binding Enter a VLAN ID if using VLANS.

***Note – If you need more than one SSID, click Add and you can create multiple.**

5GHz

Configure your 5Ghz settings.



SSID Enter the SSID. This will be visible to other devices.

Encryption Select your encryption method.

Advanced features Select if needed. **Isolate** will stop any user devices connected to this Wi-Fi from communicating with each other. **Hidden** will hide the SSID so that it is not visible.

Max Num of User Enter the maximum number of users or leave at 0 for unlimited.

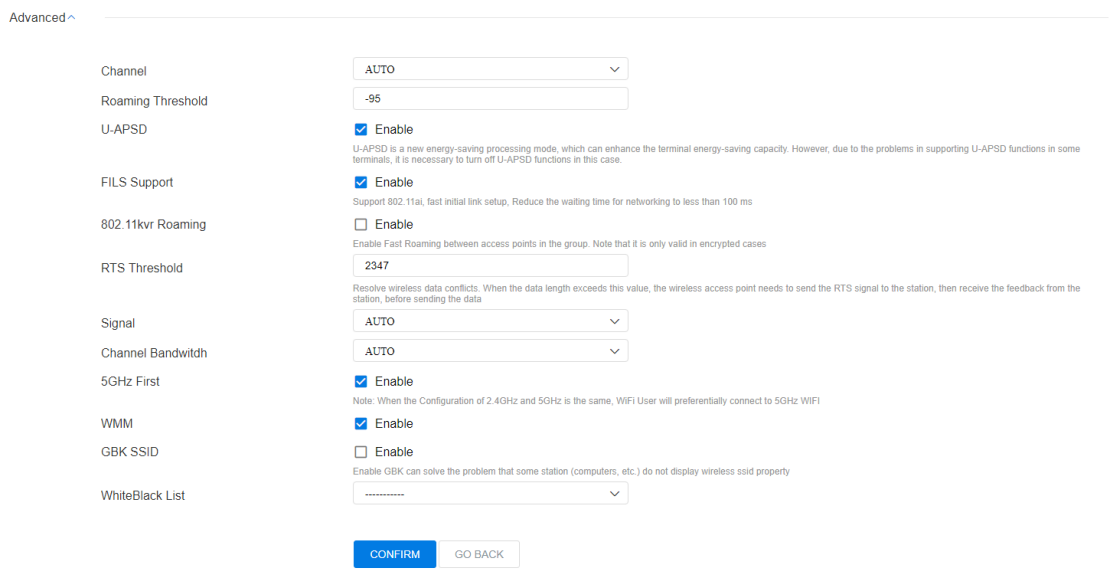
Authentication Type Select None or Local Portal.

VLAN Binding Enter a VLAN ID if using VLANS.

***Note – If you need more than one SSID, click Add and you can create multiple.**

ADVANCED

Here you can configure some advanced settings.



Channel Select the channel for your WiFi. We recommend leaving on Auto.

Roaming Threshold When a users device fall below this threshold it will automatically disconnect and roam to the next AP. Setting depends on the environment, but the recommended range is -80 to -85.

U-APSD Select Enable or Disable. U-APSD stands for Unscheduled Automatic Power Save Delivery. It is a power saving setting. When enabled any AP that does not have anything to transmit will go into standby mode checking for traffic every 100 to 200ms. Once it has something to transmit it will wake up.

This setting is fine for web browsing or emails, however, if you experience any problems then it is best to disable the setting.

FILS Support Select Enable or Disable. FILS stand for Fast Initial Link Setup. It reduces the link up time to below 100ms. Designed for dense environments.

802.11kvr Roaming Select Enable or Disable. When Enabled it allows clients to roam more seamlessly from AP to AP within the same network.

RTS Threshold Set the RTS (Request To Send) packet size. Default is 2347 octets. It is recommended to leave this setting.

Signal Set the power levels. It is recommended to leave this setting on Auto.

Channel bandwidth Set the channel size. It is recommended to leave this setting on Auto.

5GHz First Select Enable or Disable. When the configuration of 2.4GHz and 5GHz is the same, this setting will push users onto the 5GHz frequency first.

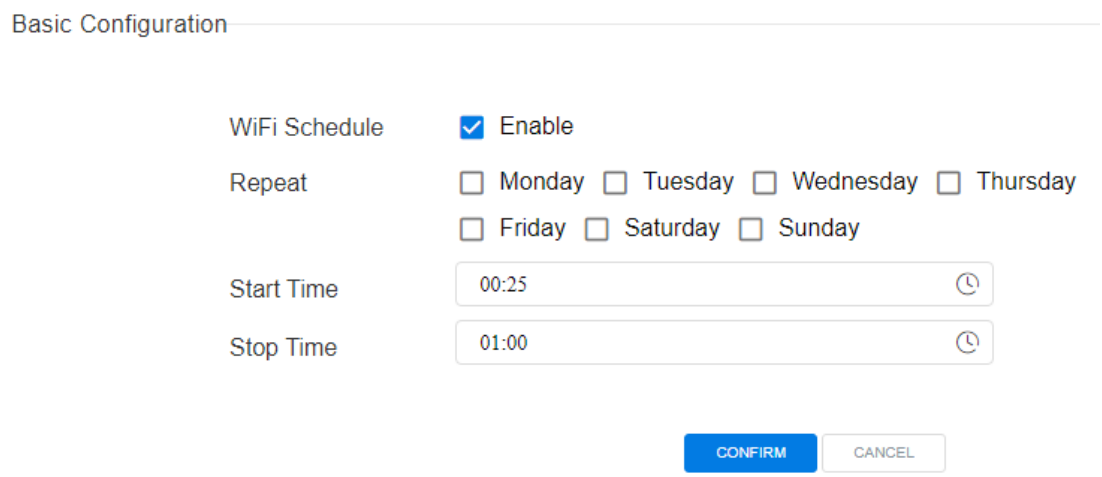
WMM Select Enable or Disable. When enabled WMM prioritises network traffic to improve performance of applications such as video and voice.

GBK SSID Select Enable or Disable. Enabling this setting can sometimes solve an issue where by some computers do not display the SSID correctly.

WhiteBlack list In White List mode, only the MAC addresses in the White list can access the WiFi. In Blacklist mode, only the MAC address in the Blacklist cannot access the WiFi. This setting is configured in its own tab. See further below.

OTHER CONFIGURATION

Configure your WiFi Schedule



WiFi Schedule Enable or Disable.

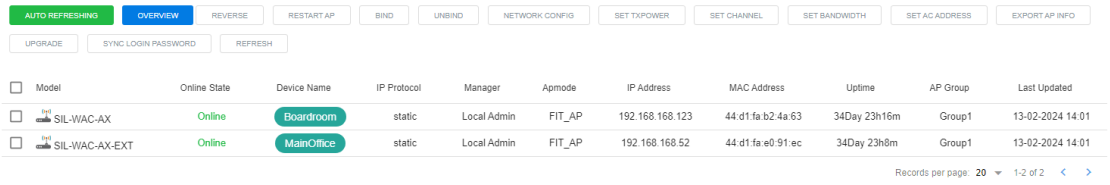
Repeat Select the days you want your WiFi Schedule to operate.

Start Time Select the start time.

Stop Time Select the end time.

AP LIST

AP List shows you the current AP's connected to the controller. To connect an AP you will need to power on the AP and make sure it is connected to the same network as the controller. Once the controller discovers the AP then it will appear as online.



BINDING

To add the online AP into the Group you simply select the AP and Click Bind. Once the AP is in the Group it will show under the AP Group column.

To unbind or to use any of the others settings (like set txpower, set channel, etc) simply select the AP and click the setting.

RF PLANNING

RF Planning can be used to scan and adjust channels.

INIT Channels Click this to use the channel plan. Save the configuration.

Start Scan This will scan and gather local WiFi information to best plan the RF channels.

Configure Click the View button to show WiFI information.

SN The AP Serial number.

Online State Online or Offline.

Plan Status Shows the initialisation channel status.

MAC Address Shows the MAC address of the AP.

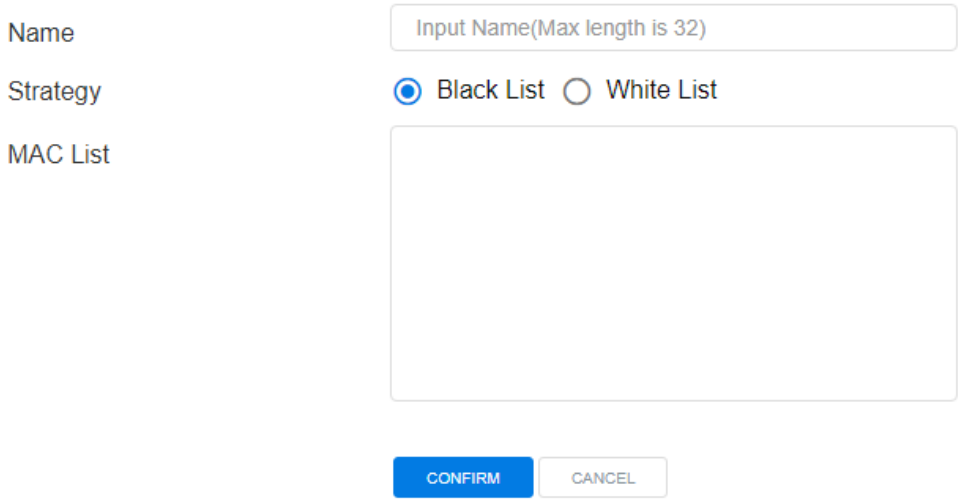
2.4GHz/5GHz Channel Shows the channel number.

2.4GHz/5GHz Noise Shows the roaming threshold.

2.4GHz/5GHz Interference Shows the number of WiFi nearby.

WHITEBLACK LIST

Click Add and choose Black List or White List.



The MAC addresses in the White list can access the WiFi. The MAC address in the Blacklist cannot access the WiFi.

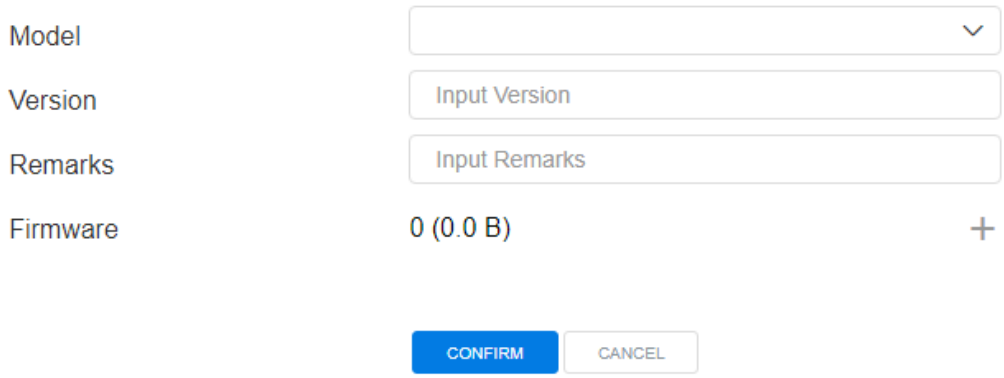
***Note - One MAC record takes up one line. You can add a note after it if separated by a space, or it can be added with no note.**

e.g., 50:00:00:00:00:01 Router MAC

e.g., 50:00:00:00:00:02

FIRMWARE

To Upgrade the firmware via the controller, the AP's must be bound in a group first.



Model Select the correct model.

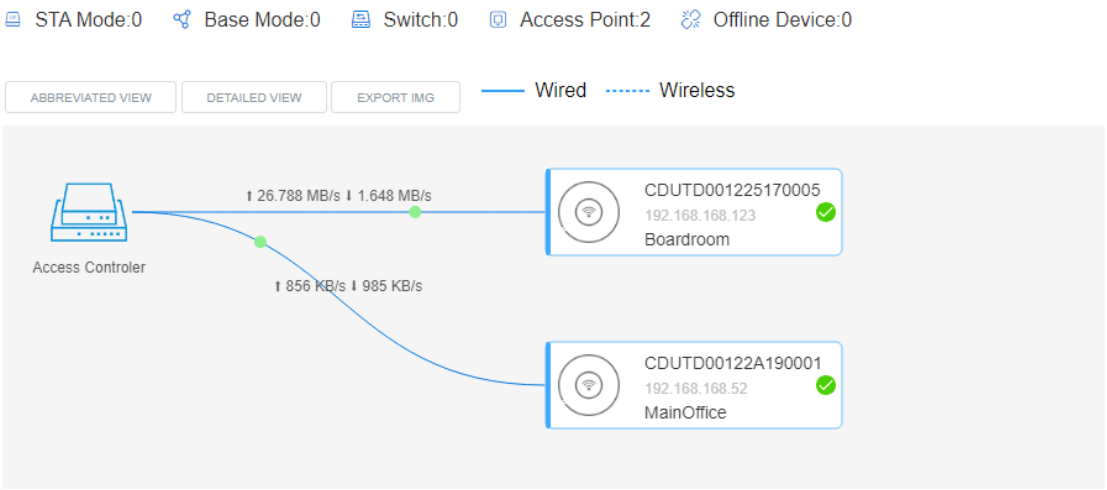
Version Input version.

Remarks Enter any remarks.

Firmware Click the + sign and browse to the firmware on your local machine.

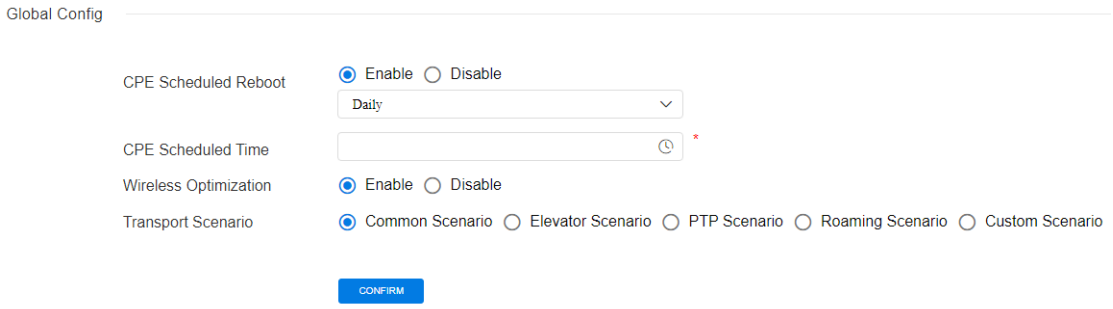
NETWORK TOPOLOGY

Displays the CPE topology such as link quality, wireless rate, current speed and CPE information in the list.



CPE MANAGEMENT

CPE GLOBAL CONFIGURATION



CPE Scheduled Reboot Enable or Disable. If Enabled, select if the schedule will be Daily, Weekly or Monthly and then Select the Day of the week or Month.

CPE Scheduled Reboot Time Select the time you wish the CPE to be rebooted.

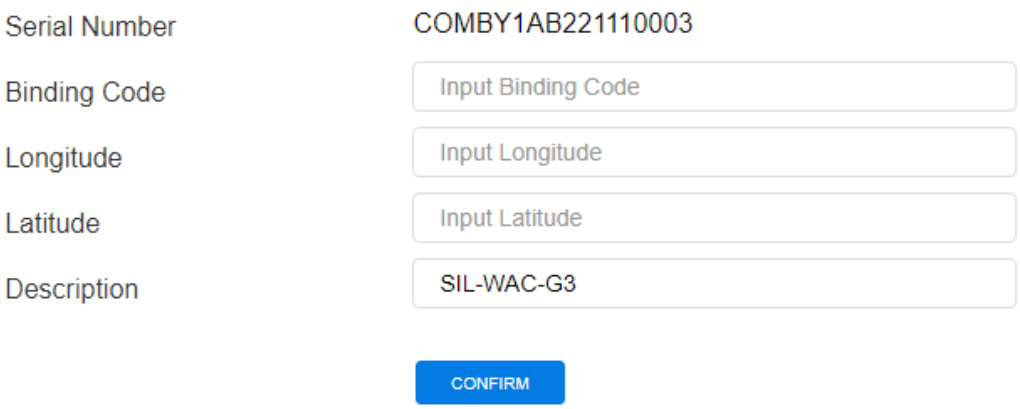
Wireless Optimisation The controller scans for any local interference and automatically assigns channels to the CPE's.

Transport Scenario Select the most suitable scenario.

UNIFIED CLOUD

UNIFIED CLOUD

Unified Cloud is a cloud platform for centralised management of wireless network devices. You can view and manage your devices in the cloud, such as: viewing the status of the devices, modifying the configuration and authentication management.



How to Bind to Unified Cloud

1.Login the Unified Cloud Control Platform -> Obtain the Binding Code -> Input the Binding Code and Note Name on Device -> Save and complete the binding.

2.Login the Unified Cloud Control Platform -> Add Group -> Add Network --> Add Device -> Input the Serial Number -> Save and complete the binding.

How to manage

After successful binding, about 3 minutes, you can see the device in the Unified Cloud, which can be managed and on Unified Cloud.

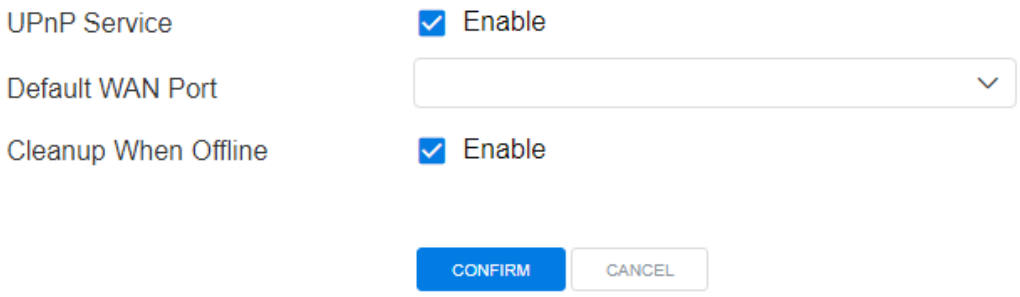
How to unbind with Unified Cloud

Login to the Unified Cloud, on the Routing List - > Device Management - > Routing Information Overview Page, you can unbind the device.

APPLICATION

UPNP SERVER

Universal Plug and Play (UPnP) is a standard that lets network devices automatically find, communicate, and control each other. You can enable UPnP in this section.



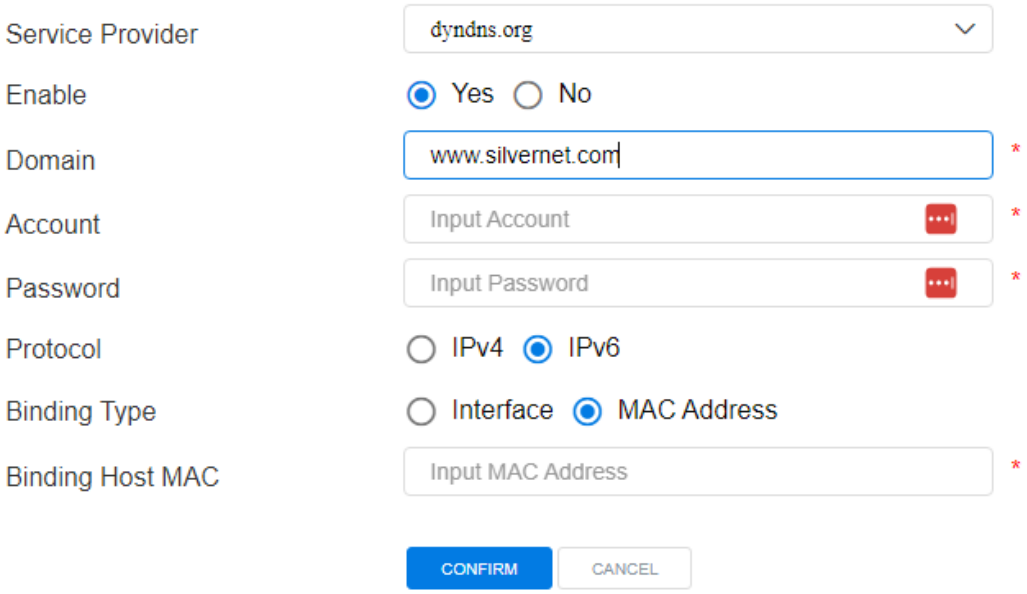
UPnP Service Enable or Disable.

Default WAN Port WAN

Cleanup When Offline Enable or Disable.

DDNS

Dynamic DNS (DDNS) is a service that can automatically update DNS records when an IP address changes. It connects to the DDNS service providers system with a unique login name and password. Depending on the provider, the host name is registered within a domain owned by the provider or within the customers own domain name. For detailed configuration parameters, please contact the service provider.



Service Provider Select a service provider from the list.

Enable Enable or Disable.

Domain Enter the domain name.

Account Enter the account information.

Password Enter the Password information.

Protocol Select IPv4 or IPv6.

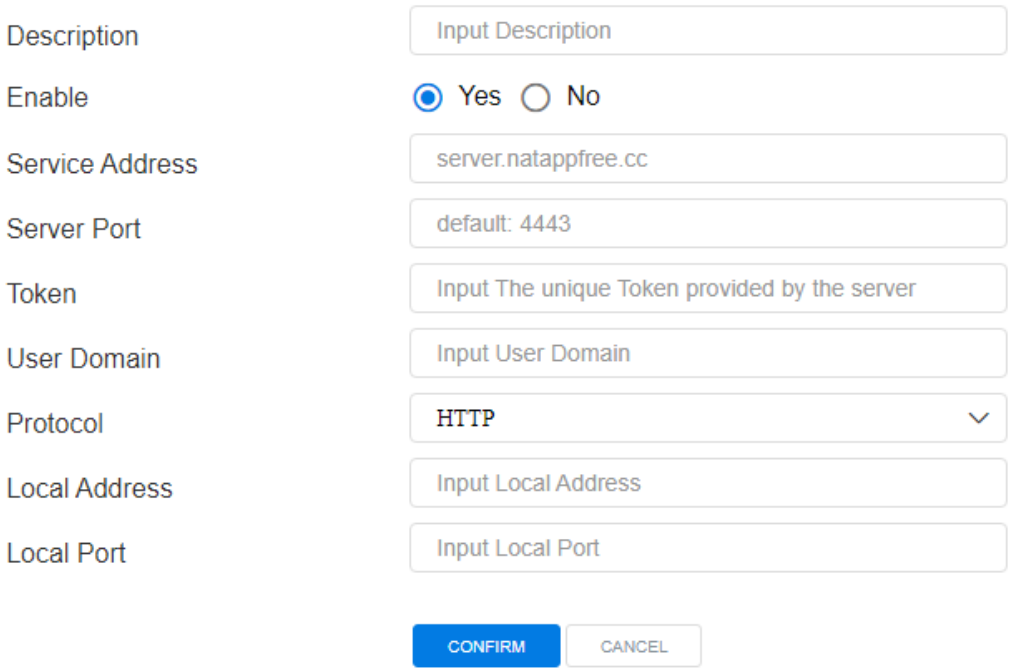
Binding Type Select interface or MAC address.

Binding Host MAC Input the MAC address.

Binding Interface Select the binding interface.

NGROK CLIENT

Ngrok allows you to create a managed tunnel that does not need NAT or port mapping.



Description Enter a description.

Enable Yes or No.

Service Address Enter the server address.

Server Port Default is 4443

Token Enter the unique token provided by the server.

User Domain Enter the user domain.

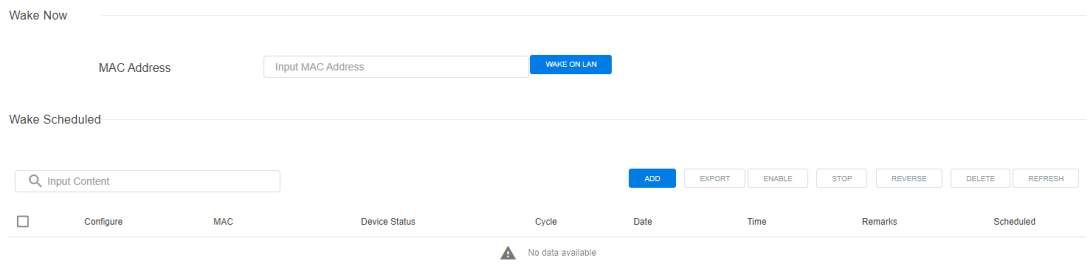
Protocol Select HTTP, HTTPS, TCP.

Local Address Input the local address

Local Port Input the local port.

WAKE ON LAN

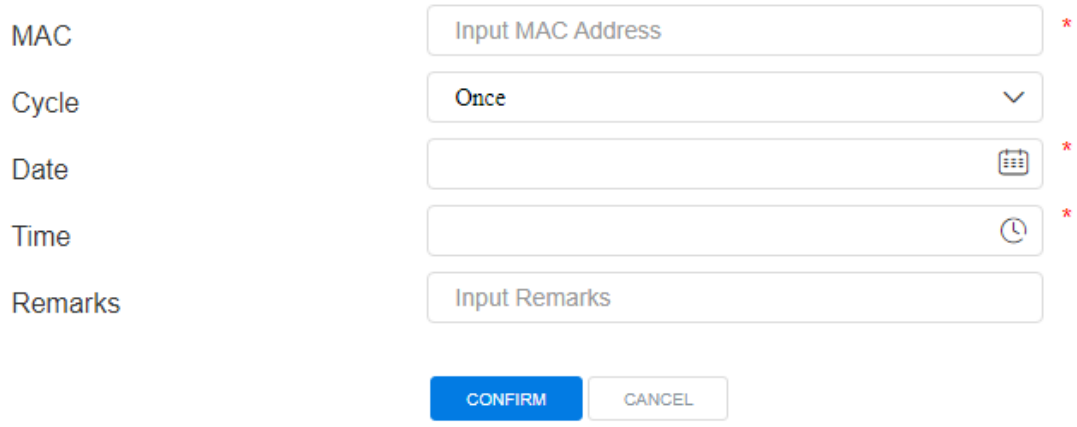
Wake-on-LAN (WOL) is an Ethernet or token ring computer networking standard that allows a computer to be turned on or awakened by a network message. The message is usually sent to the target computer by a program executed on a device connected to the same local area network, such as a smart phone.



Wake Now

MAC Address Enter the MAC address of the device to wake up.

Wake Schedule



MAC Enter the MAC address of the device to Wake up.

Cycle Select once, daily, weekly or monthly.

Date Select the date.

Time Select the time.

Remarks Enter any remarks.

Switch Linkage

Here you can use SNMP to add switches to the controller for management and monitoring.

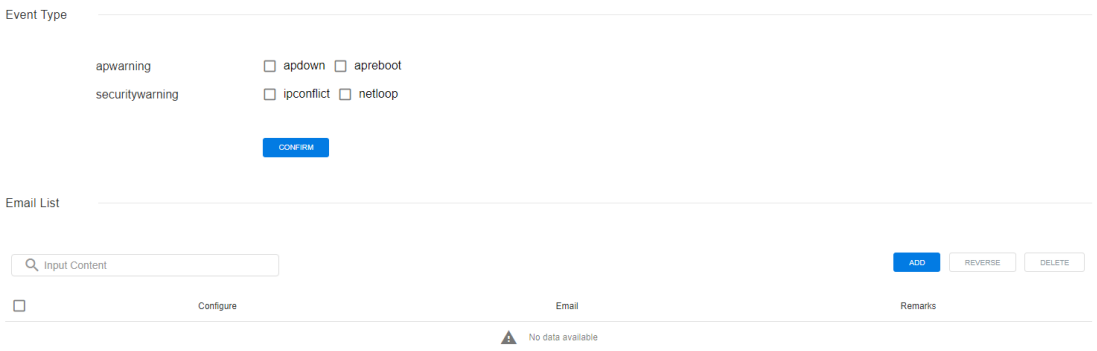
Smart Device

Here you can use manage and monitor devices like cameras, etc.

Security

Email Notice

Email notice only works when using a cloud option. It does not work without access to the cloud.



Click add to enter an email address. Select the Events you wish to receive an email for.

System

This section is where you can change the system name, save config files, etc.

System Maintenance

System Information

Device Name Enter a name.

Reboot

Uptime Shows the uptime of the controller.

Reboot Click reboot now to reboot the controller.

Online upgrade

Check for new version Will check online for a newer version of firmware.

System Version Displays the current version of firmware.

Model Displays the model number.

Serial Number Displays the serial number.

Menu Upgrade

Local Upgrade Click the + sign and browse to the firmware on your local machine.

Upload Backup File

Last Backup Time Shows the last time a backup configuration file was saved.

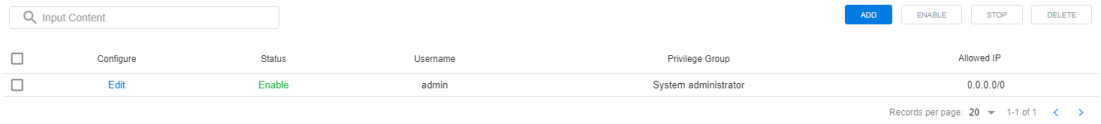
Upload Backup file Click the + sign and browse to the configuration file on your local machine.

Backup Configuration Click this to save the current configuration file.

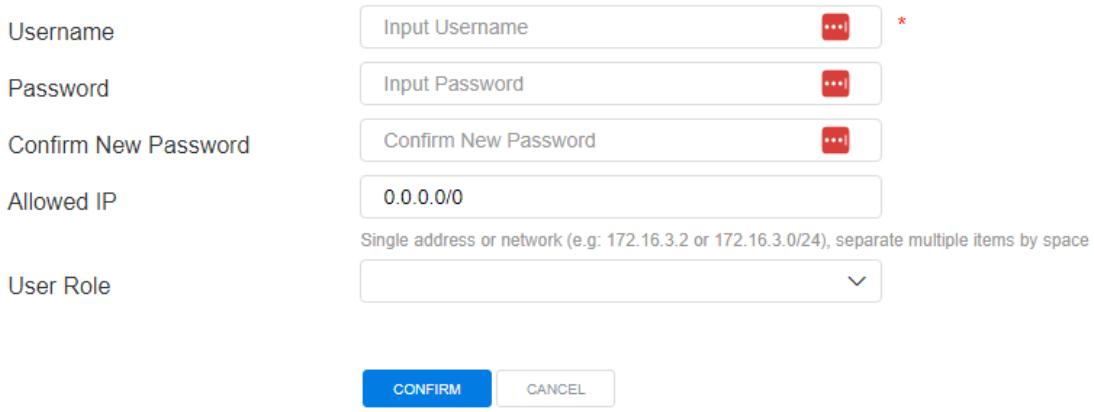
Reset to Factory Click this to reset the controller to its factory default settings.

USER MANAGEMENT

This section allows you to add and remove users.



Click Add to add a new user or Edit to change the administrator details.



Username Enter a username

Password Enter a password

Confirm New Password Re-enter the password.

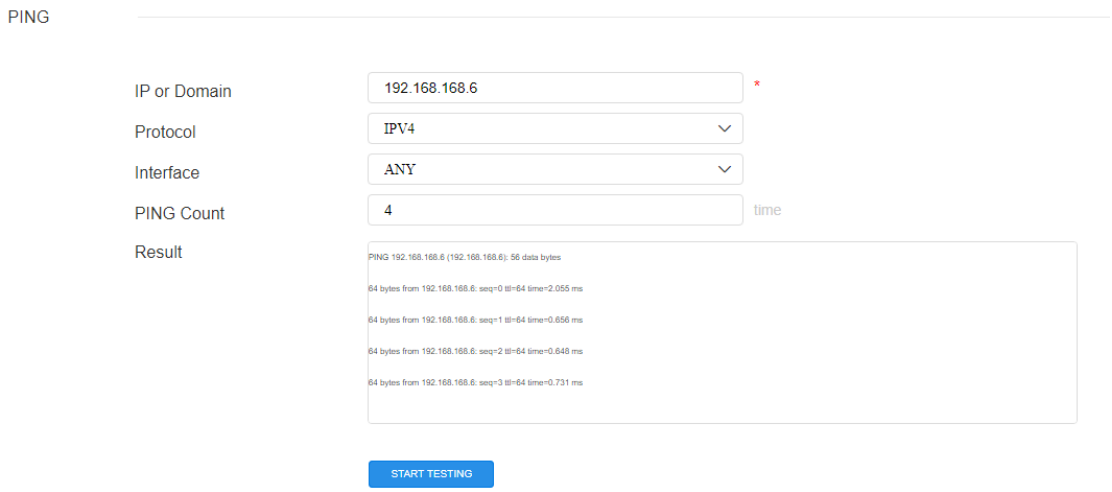
Allowed IP This allows access to certain IP addresses.

User Role Select the role of the user. Admin account defaults to administrator.

DIAGNOSIS

Here you can run a ping test and a traceroute test.

PING



IP or Domain Enter the IP address or Domain you wish to ping.

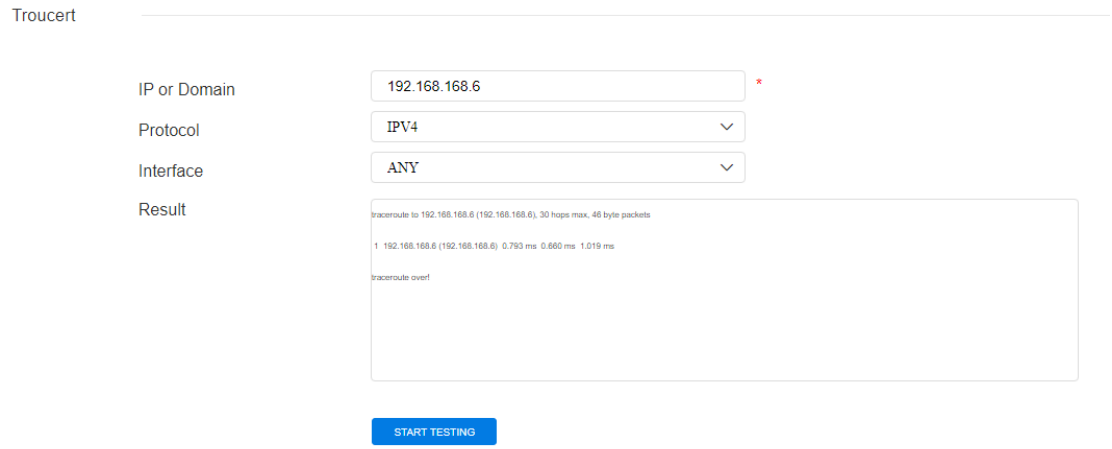
Protocol Select the protocol you wish to use.

Interface Select the interface.

Ping Count Select the amount of pings

Start test Starts the ping test.

TRACEROUTE



IP or Domain Enter the IP address or Domain you wish to ping.

Protocol Select the protocol you wish to use.

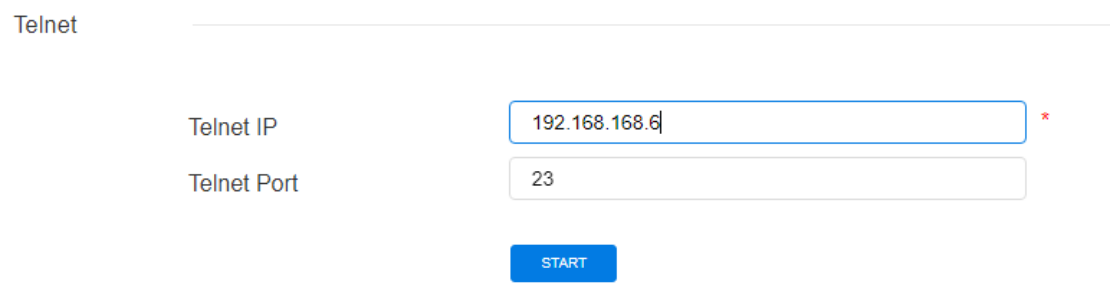
Interface Select the interface.

Start test Starts the ping test.

NETWORK TOOL

Here you can use this section to access the telnet of devices like switches.

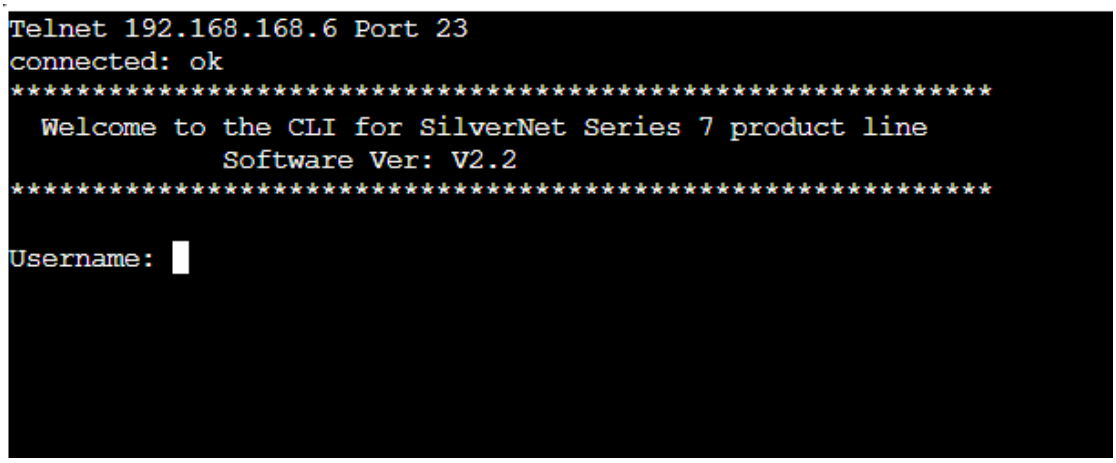
TELNET



Telnet IP Enter the IP address or Domain you wish telnet to.

Telnet Port Enter the telnet port.

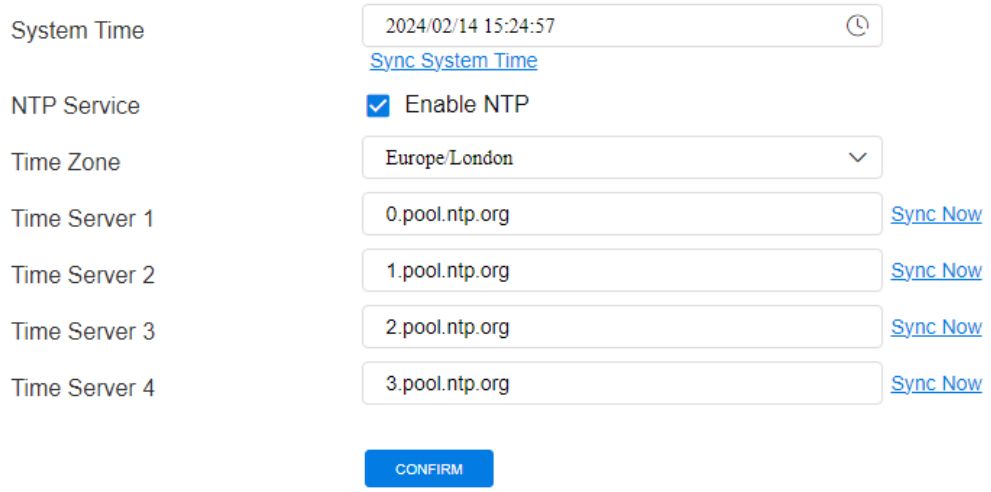
Click start to open the session.



System Time

This is where you can set up your NTP. The Controller automatically updates the system time once it has internet access.

NTP



System Time Displays the current time.

NTP Service Enable or Disable NTP.

Time Zone Select your time zone.

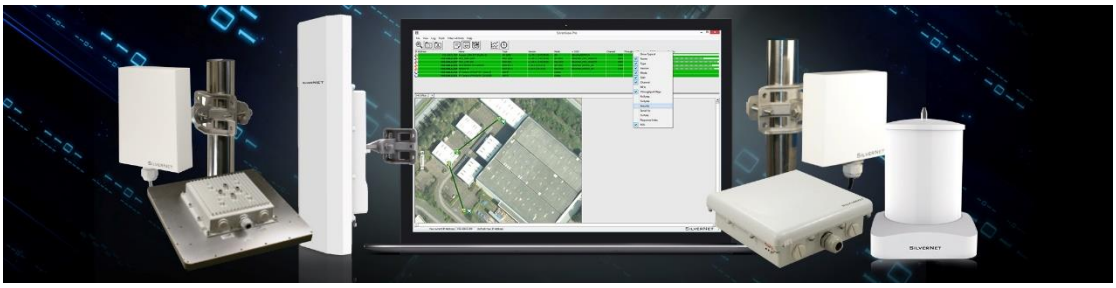
Time Server Enter details of your time server and Sync.

Logging

This is where you can see and export any logs for diagnostics.

OTHER SILVERNET PRODUCTS

PRO RANGE



INDUSTRIAL NETWORK TRANSMISSION

INTELLIGENT WI-FI SOLUTIONS

INDUSTRY LEADING TECHNICAL SUPPORT